Groupe de travail
Sécurité des systèmes
d'information de santé

Etude de la réglementation et des recommandations relatives à la sécurité des systèmes d'information de santé

Mars 2004

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, Rue Pierre Sémard – 75009 Paris
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

Remerciements

Le CLUSIF remercie ceux qui ont participé à la rédaction de ce document :

ATTAL Gérard	AMACOM
CARLI-BACHER Sophie	GMSIH
CRETON Philippe	SCHEDIR
De CADEVILLE Anne	XP-CONSEIL
DLUGOSZ Gilles	FEHAP
FAIDHERBE Georges	GESTIC
JANIN Samuel	SILICOMP
PARROT Daniela	CNIL
PEJSACHOWICZ Lazaro	CNAMTS
SEDALLIAN Valérie	AVOCAT

Ainsi que tous ceux qui, par leur présence assidue, ont contribué aux travaux du Groupe de Travail Santé :

CHAUVOT Frédéric	GIE SESAM VITALE
FERRAND Christian	CLUSIR LANGUEDOC-ROUSSILLON
HARLE Thierry	BSGL
MOLINES Gérard	MOLINES CONSULTANTS
TALLOT Christophe	PRICEWATERHOUSECOOPERS
TROUESSIN Gilles	ERNST & YOUNG

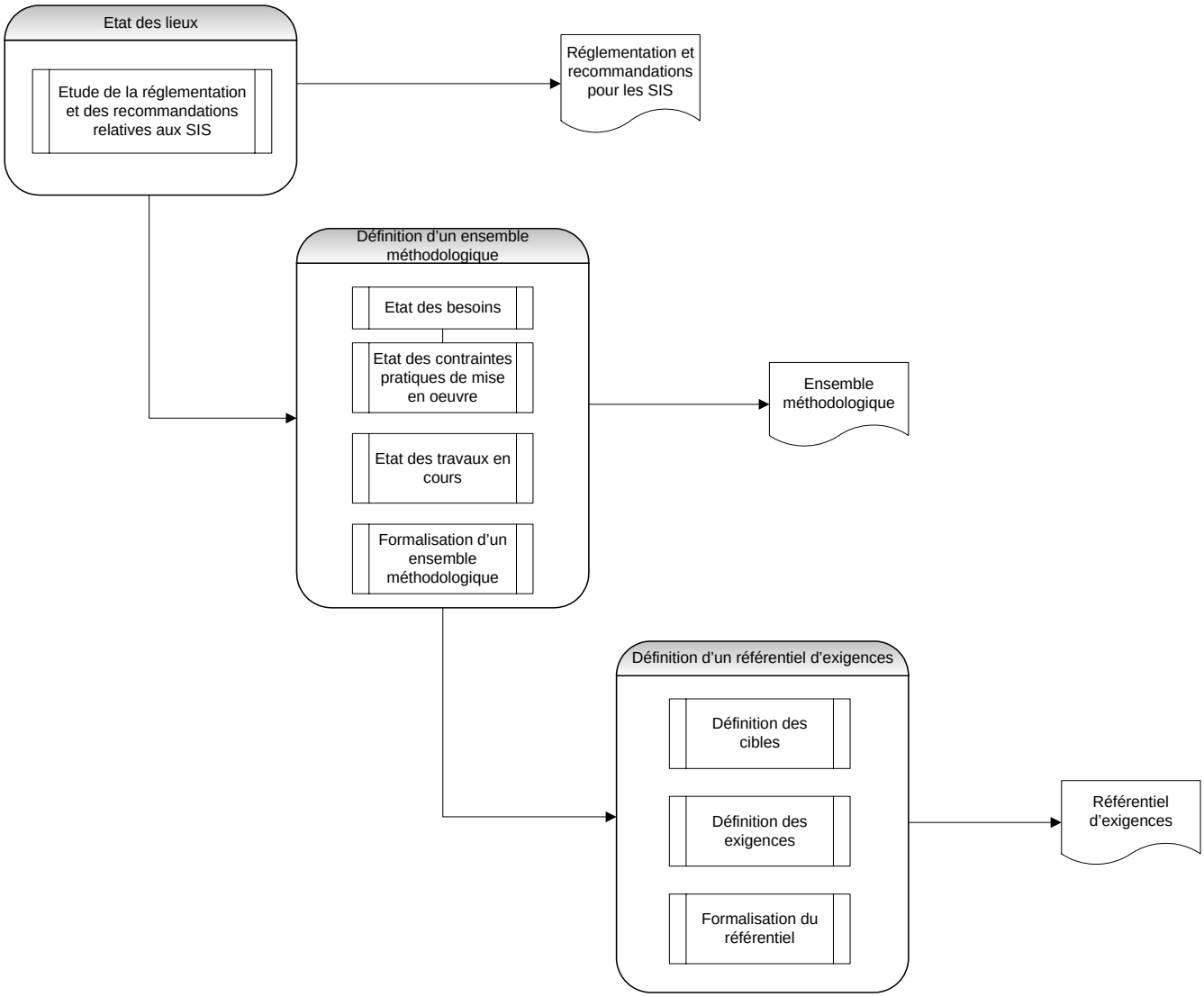
Table des Matières

1 Concepts 7
1.1 L'hébergement des données de santé 7
1.2 Preuve, traçabilité, auditabilité 8
1.3 Le concept de vie privée 8
2 Synthèse des fiches de lecture 11
2.1 Les textes juridiques et réglementaires 11
2.1.1 Le traitement des données personnelles 11
2.1.2 Les données du système d'information de santé 12
2.1.3 Les atteintes aux systèmes informatiques 12
2.2 Les textes techniques 12
2.2.1 Les normes ISO 13
2.2.2 Les normes du CEN 14
2.2.3 Les normes AFNOR 14
2.2.4 Les recommandations 14
2.2.5 Les études 14
2.2.6 La méthode MEHARI du CLUSIF 15
2.3 Les implications de la loi du 4 mars 2002 16
2.4 Les implications de la nouvelle loi de transposition 17
3 Liste des textes, références et documents applicables 18
4 Annexe 1 : Recueil des fiches de lectures validées par le GT 21
A.1.1 Référentiels, normes et recommandations techniques 21
A.1.2 Protection des données personnelles 41
A.1.3 Certification et contrôle 64
A.1.4 Protection contre la fraude 72
A.1.5 Confidentialité et secret professionnel 76
A.1.6 Textes généraux 79

Préambule

Ce document s'inscrit dans une réflexion globale sur le besoin de sécurité des systèmes d'information de santé.
Il a été formé au CLUSIF, dans ce but, un groupe de travail dont la mission est de mener à bien cette réflexion.

La démarche du groupe de travail santé est la suivante :



Ce document ne prend en compte que les textes et recommandations publiés officiellement jusqu'à la date du 22 juillet 2003, début de son élaboration.

Celui-ci est appelé à évoluer, en fonction de la contribution des membres du groupe de travail, des publications et de la législation.

Une nouvelle version sera rédigée pour juillet 2004, complétée des derniers textes juridiques.

L'objectif de ce document est de fournir une base commentée, la plus complète possible, des aspects législatifs, réglementaires et des recommandations relatives à la sécurité des systèmes d'information de santé.
Cette étude servira de base pour la définition d'un ensemble méthodologique destiné à évaluer et piloter la sécurité des systèmes d'information de santé dans le cadre des réseaux constitués entre tous les organismes et professionnels de santé.

Le champ d'application de ce document est l'ensemble des établissements et organismes qui traitent de la santé humaine, de façon directe (établissements de soins, hôpitaux, cliniques, cabinets médicaux,...) ou indirecte (organismes d'assurance sociale, mutuelle de santé, ...).

Ce document comprend trois parties et une annexe :

Chapitre 1 :	définition des concepts
Chapitre 2 :	Synthèse des fiches de lecture
Chapitre 3 :	Liste des textes applicables
Annexe :	Recueil des fiches de lectures validées par le Groupe de Travail

Glossaire

ACI	(Availability/Confidentiality/Integrity) Disponibilité/Confidentialité/Intégrité.
AFNOR	Association Française de Normalisation.
ANAES	Agence Nationale d'Accréditation et d'Evaluation en Santé.
CEN	Comité Européen de Normalisation.
CSP	Code de la Santé Publique.
CSSI	Comité de Sécurité du Système d'Information.
COSSI	Comité Opérationnel de Sécurité du Système d'Information.
DIM	Département d'Informatique Médicale.
DIP	Droits et Information du Patient.
DPA	Dossier du Patient.
GMSIH	Groupement pour la Modernisation du Système d'Information Hospitalier.
GSI	Gestion du Système d'Information.
GTESSI	Groupe de travail pour l'étude de la sécurité du système d'information.
HCE	(Healthcare Establishment) Établissement de santé.
HCIS	(Healthcare Information Systems) Systèmes d'information de santé.
ISO	International Organization for Standardization.
LAN	(Local Area Network) Réseau local.
LCA	(Logical Connectivity Assumption) Hypothèse de connectivité logique.
OPC	Organisation de la prise en charge des patients.
PC	(Personal Computer) Ordinateur individuel.
PCA	(Physical Connectivity Assumption) Hypothèse de connectivité physique.
PEA	(Physical Environment Assumption) Hypothèse d'environnement physique.
PMSI	Programme de Médicalisation des Systèmes d'Information.
PP	(Protection Profile) Profil de protection.
RNIS	Réseau Numérique à Intégration de Services.
RSS	Réseau de santé sociale.
RSSI	Responsable de la Sécurité des Systèmes d'Information.
RSV	Réseau Sésame Vitale.
SSE	Sous système étendu.
SSR	Sous système restreint.
SI	Système d'Information.
SIH	Système d'Information Hospitalier.
SIS	Système d'Information de Santé.
SDSI	(ou SDI) Schéma Directeur des Systèmes d'Information.
SDSSI	Schéma Directeur de la Sécurité des Systèmes d'Information.
SU	(Small User) Petit utilisateur.
TI	(Information Technology) Technologies de l'information.
TLSO	(Top Level Security Objectives) Objectifs de sécurité de niveau maximal.

1 Concepts

Ce chapitre a pour objet de clarifier les quelques concepts et principes manipulés dans ce document et qui ont besoin d'être précisés au préalable.

1.1 L'hébergement des données de santé

➢ L'article L. 1111-8 du CSP issu de la loi du 4 mars 2002, prévoit que les données de santé recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins peuvent être déposées par les professionnels de santé, les établissements ou les patients auprès d'une personne physique ou morale agrée à cet effet. Cet hébergement ne peut avoir lieu qu'avec l'accord exprès de la personne concernée.
La prestation d'hébergement qui consiste principalement en l'organisation du dépôt, la conservation des données et leur mise à disposition doivent faire l'objet d'un contrat spécifique. Ce contrat doit notamment prévoir, lorsque le professionnel de santé ou l'établissement est à l'origine de l'hébergement, que l'hébergement des données, les modalités d'accès et de transmission soient subordonnées à l'accord de la personne concernées. Les données ne peuvent être utilisées à d'autres fins que celles définies dans le contrat d'hébergement.

Le traitement doit être réalisé conformément à la loi "Informatique et Libertés".

Les patients disposent d'un droit d'accès auprès de l'hébergeur ainsi que les professionnels de santé et les établissements de santé qui les prennent en charge et qui sont désignés par les personnes concernées (les patients).

➢ Les conditions de l'agrément doivent être fixées par décret en Conseil d'Etat pris après avis de la CNIL et des conseils de l'ordre des professions de santé et des professions paramédicales.

Ce décret précise les informations à fournir à l'appui de la demande d'agrément, les modèles de contrats de prestation d'hébergement, les dispositions prises pour garantir la sécurité des données traitées et en particulier les mécanismes de contrôle et de sécurité informatique ainsi que les procédures de contrôle interne.

➢ L'agrément peut être retiré en cas de violation des prescriptions législatives ou réglementaires relatives à cette activité ou des prescriptions fixées par l'agrément.

Les hébergeurs sont astreints au secret professionnel (article 226-13 du code pénal) et sont soumis au contrôle de l'Inspection générale des affaires sociales.

➢ Lorsqu'il est mis fin à l'hébergement, l'hébergeur restitue les données, sans garder de copie, au professionnel, à l'établissement ou à la personne concernée ayant contracté avec lui.

➢ Le fait d'héberger de données de santé à caractère personnel sans être titulaire de l'agrément ou de traiter ces données sans respecter les conditions de l'agrément obtenu est puni de trois ans d'emprisonnement et de 45 000 € d'amende.

➢ A ce jour aucun décret n'est intervenu. Le contour de la notion d'hébergeur de données de santé reste flou. Les réseaux de soins, dont les données seront hébergées par l'un des établissements participant au réseau, devront-ils être agréés ? Les organismes concentrateurs techniques (OCT), chargés de télétransmettre pour le compte des professionnels de santé les feuilles de soins électroniques, les tiers de confiance visés dans le rapport Babusiaux sur l'accès des assureurs aux données de santé des feuilles de soins électroniques seront-ils concernés par l'agrément ?

1.2 Preuve, traçabilité, auditabilité

Dans le monde de la santé le besoin de preuve et de traçabilité des opérations – y compris des opérations de consultation des dossiers - devient une exigence nécessaire.

Il est proposé de reformuler en premier lieu les exigences de sécurité que recouvrent ces notions :

- pouvoir disposer d'un système auditable et tracer/retracer des évènements (des actions) en vue d'exercer une supervision (surveillance), un contrôle ou de mener des investigations a posteriori,
- pouvoir fournir une preuve dite interne, c'est-à-dire un ensemble reconnu d'éléments de preuve en vigueur dans une communauté (un établissement, un secteur d'activité,…), et opposable en cas de litige,
- pouvoir fournir une preuve dite externe, ou preuve difficilement contestable, dans la mesure où la loi fixe les éléments de preuve à fournir (la signature électronique avec des certificats qualifiés par exemple).

Dans le monde de la santé les enjeux sont importants :

- apporter les moyens de preuve et de contrôle nécessaires aux utilisateurs (professionnels de santé, …) et aux patients pour accorder leur confiance dans l'information fournie,
- sur un plan plus général, permettre une véritable dématérialisation des relations contractuelles et administratives.

Dès lors, les mécanismes de preuve et de contrôle peuvent se décliner de la manière suivante :

- l'audit : le système d'information doit être auditable au niveau du paramétrage des composants techniques, de son organisation et des processus qu'il génère,
- la trace : le système d'information doit générer des traces permettant de suivre le cheminement des informations au sein des processus et de mener des analyses approfondies, a posteriori,
- la non répudiation : l'émetteur et le destinataire d'une information ne doivent pas pouvoir nier l'avoir émise ou reçue, ni contester son contenu. L'appel à un tiers de confiance (un "notaire") garantissant l'existence et le contenu d'un échange doit être prévu, si nécessaire,
- l'imputation : le système d'information doit permettre d'attribuer une action à un acteur clairement identifié.

1.3 Le concept de vie privée

1) au plan juridique : de la protection des données à caractère personnel à celle de la vie privée

La CNIL a été créée, entre autres, pour lutter contre les interconnexions abusives de fichiers informatiques contenant des données à caractère personnel, cependant la personne privée, en l'occurrence le patient, peut légitimement craindre désormais que les nombreuses traces enregistrées par les fournisseurs d'accès, les entreprises et les administrations, ne viennent compromettre la protection de sa vie privée.

Cette protection de la vie privée est traitée dans le Code Civil :

"Chacun a droit au respect de sa vie privée.
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé. "

Le cas d'abus par les medias en est un exemple. Ainsi peut-on citer la jurisprudence « Chantal Nobel » qui fait reconnaître, en condamnant des journalistes, que la chambre d'hôpital est un lieu privé : c'est le droit de la personne au respect de son intimité.

La protection de la vie privée, est également abordée par la Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

Dans le secteur de la santé, la Loi du 4 mars 2002 stipule dans son article 3 que « toute personne prise en charge par un professionnel, un établissement, un réseau de santé ou tout autre organisme participant à la prévention et aux soins a droit au respect de sa vie privée et du secret des informations la concernant » (article L. 1110-4 du Code de la Santé Publique)

2) au plan méthodologique, l'exigence de la « protection de la vie privée » ne peut être uniquement portée par le concept de confidentialité des informations.

La loi du 4 mars 2002 nous apporte un certain nombre de réponses, qui devraient être précisées par décret :

- notion de « patient-acteur », patient qui accorde ou retire le droit à un professionnel de santé de consulter son dossier,
- communication du dossier au patient sur sa demande (communication directe rendue possible)
- décrets particuliers couvrant la communication des données médicales d'un patient entre structures et professionnels, sécurité de l'hébergement de dossiers médicaux,…

En faisant un parallèle pour la santé avec les principes plus généraux qui protègent le citoyen, on pourrait avancer que la protection de la vie privée du patient couvre les aspects suivants :

- le droit au secret des informations personnelles, lors des traitements automatisés et lors des échanges de données,
- le droit à l'anonymat (protection des VIP, des malades atteints de pathologies pour lesquelles l'anonymat est requis, mais aussi protection de tous lorsque des traitements statistiques ou épidémiologiques sont réalisés – type PMSI –),
- les droits inscrits dans la Loi Informatique et Libertés : droit à l'information préalable, droit d'accès et de rectification, droit d'opposition, droit à l' « oubli »,

- le droit à détenir des droits sur ses informations personnelles (qui représentent autant de limites pour les détenteurs de données personnelles),
- les limites légales concernant la traçabilité des opérations (télécommunications,…)

2 Synthèse des fiches de lecture

Il existe deux types de textes qui ont été étudiés dans ce document :

- les textes juridiques et réglementaires : des lois, des décrets, des directives, ...
- les textes techniques : des études, des recommandations, des normes, ...

Certains de ces textes techniques ont une force réglementaire par le caractère obligatoire que leur confère la loi.
ex : les recommandations de l'ANAES qui sont rendues obligatoires dans le code de la santé publique

2.1 Les textes juridiques et réglementaires

Il existe trois catégories de textes :

- Les textes encadrant le traitement des données personnelles
- Les textes encadrant le système d'information de santé
- Les textes réprimant les atteintes aux systèmes informatiques

2.1.1 Le traitement des données personnelles

Les textes encadrant les données personnelles en France (loi 78-17 dite loi Informatique et Libertés) sont anciens et doivent être prochainement remplacés. Une nouvelle loi remplacera la loi actuelle.
La France a obligation de légiférer dans ce domaine et de produire une loi dite "de transposition" qui reprend la directive Européenne 95-46.
Cette nouvelle loi "de transposition" est en cours d'adoption et devrait être votée prochainement (cf paragraphe : 2.4 les implications de la nouvelle loi de transposition).

Le code pénal dans ses articles 226-16 à 24 réprime les infractions relatives au traitement des informations personnelles.

Les textes relatifs à la protection des données personnelles et au respect de la vie privée sont à l'origine de la nécessité de la mise en oeuvre de la "charte d'utilisation des moyens informatiques" dans les organismes publics ou privés.

2.1.2 Les données du système d'information de santé

Les textes encadrant le système d'information de santé sont publiés dans les documents suivants :

- le code de déontologie médicale

  Ce texte précise la notion de secret médical, les obligations du médecin vis à vis du secret médical et de sa protection.

- le code de santé publique, modifié par la loi Kouchner (2002-303du 4 mars 2002) avec son décret d'application (2002-637 du 29 avril 2002).

  Ce texte modifie et précise les rapports entre le médecin et le patient. (cf paragraphe 2.3 les implications de la loi du 4 mars 2002).
  Deux décrets d'application de cette loi doivent encore être rédigés.
  Le premier concerne la réglementation relative à l'hébergement des données de santé. Ce texte devrait sortir au début de l'année 2004.
  Le second concerne la politique de confidentialité et dépend en partie de la loi de transposition. Il ne sortira qu'après l'adoption de cette dernière loi.

  Le projet de loi relatif à la politique de santé publique devrait encore modifier le code de santé publique et le code de la sécurité sociale, en particulier l'article 13 relatif au système d'information.

- la recommandation No.R (97) 5 du conseil de l'Europe

  Ce texte précise les recommandations relatives à la protection et au recueil des données médicales.

- le code de la sécurité sociale

  Ce texte précise les données de santé (directes ou indirectes) qui peuvent être traitées, les conditions dans lesquelles elles doivent être traitées, les moyens et précautions à prendre.

2.1.3 Les atteintes aux systèmes informatiques

Les atteintes aux systèmes informatiques sont précisées par le code pénal dans les articles 323-1 à 7.

Le projet de loi portant adoption de la Convention sur la cybercriminalité signée le 23/11/2001 à Budapest (Conseil de l'Europe) autorise l'adoption de la Convention qui précise complètement les principes de la lutte contre la cybercriminalité et le besoin de protéger les intérêts légitimes liés au développement des technologies de l'information.

2.2 Les textes techniques

Les textes techniques se répartissent en trois catégories :

- les normes qui sont un cadre commun de définition des principes et pratiques relatifs à la SSI
  - Les normes peuvent se distinguer entre les normes de portée mondiale (ISO), européenne (CEN) et nationale (AFNOR).

- On peut encore distinguer les normes européennes expérimentales ou provisoires (qui peuvent être contredites par des normes nationales) et les normes validées qui ont une vocation à supplanter les normes nationales.

- les recommandations émises par divers organismes
  - Ces recommandations ont une portée locale et ne peuvent se substituer aux normes nationales ou européennes.

- les études réalisées par divers organismes
  - Ces études n'ont aucune valeur de recommandation et ne s'imposent que par la qualité des travaux qui les constituent.

2.2.1 Les normes ISO

Il n'existe pas de norme ISO traitant de la sécurité des systèmes d'information de santé.
Ce type de texte reste très difficile à produire du fait de la forte implication du contexte juridique national qui diffère beaucoup suivant les pays, en particulier entre les Etats Unis et l'Europe.

Les normes qui traitent de la sécurité des systèmes d'information ont une portée plus générale et s'appliquent à tous les organismes qui traitent des informations sensibles.

Ce sont les normes suivantes :

ISO 15408 : critères communs

Les Critères Communs présentent les exigences concernant la sécurité d'un produit ou d'un système sous deux formes distinctes : les exigences fonctionnelles et les exigences d'assurance.
Les exigences fonctionnelles des Critères Communs définissent le comportement de sécurité souhaité : elles décrivent les fonctionnalités de sécurité que peut mettre en oeuvre un produit.
Les exigences d'assurance constituent la base pour acquérir la confiance dans le fait que les mesures de sécurité sont conformes aux spécifications et sont efficaces.

ISO 17799

L'ISO/ CEI 17799 transforme la Norme britannique BS 7799, qui a été adoptée dans de nombreux pays, en une norme internationale qui tend à devenir un document de référence pour les pratiques relatives à la SSI.

ISO 13335

Cette norme est un document qui définit les lignes directrices pour la gestion de la sécurité des technologies de l'information (TI) en 5 parties :

Partie 1: Concepts et modèles pour la sécurité des TI
Partie 2: Management et planning de sécurité TI
Partie 3: Techniques pour la gestion de sécurité TI
Partie 4: Sélection de sauvegardes
Partie 5: Guide pour la gestion de sécurité du réseau

2.2.2 Les normes du CEN

Le CEN/TC 251 a publié un ensemble de documents normatifs qui définissent les règles relatives à la sécurité des systèmes d'information de santé :

ENV 12924 : Security Categorisation and Protection for Healthcare Information Systems

ENV 13606 : Electronic healthcare record communication
- Part 1: Extended architecture
- Part 2: Domain termlist
- Part 3: Distribution rules
- Part 4: Messages for the exchange of information

ENV 13608 : Security for healthcare communication
- Part 1: Concepts and terminology
- Part 2: Secure data objects
- Part 3: Secure data channels

ENV 12251 : Secure User Identification for Healthcare

ENV 13729 : Secure user identification for healthcare strong authentication using microprocessor cards

2.2.3 Les normes AFNOR

L'AFNOR a intégralement repris et publié les normes du CEN : 12924,13606 et 13608.
Ces normes sont expérimentales et doivent encore obtenir le statut de normes définitives pour être complètement applicables.

Une révision de ces normes doit intégrer les retours d'expérience de la mise en oeuvre.

2.2.4 Les recommandations

L'ANAES a publié un ensemble de recommandations dont les critères applicables au système d'information mentionnent simplement la nécessité de sécuriser le système d'information.

L'ANAES devrait publier une nouvelle version des recommandations prenant en compte de façon plus formelle les contraintes liées à la sécurité du système d'information de santé.

Les recommandations de l'ANAES ont un caractère obligatoire et sont évaluées par des experts qui visitent les établissements pour vérifier la bonne mise en oeuvre des recommandations.

La CNIL a publié un guide précisant les recommandations relatives au traitement des données de santé par les professionnels de santé.

2.2.5 Les études

Le GMSIH a publié des études sur la sécurité des systèmes d'information.
Ces études sont récentes, et il n'existe pas encore de retour d'expérience sur leur mise en oeuvre.

Ces études sont les suivantes :

Si51PSC1,2,3	politique de sécurité cadre pour les systèmes d'information

Si51PAU1,2	politique d'autorisation pour les systèmes d'information
Si51GAE	guide d'auto-évaluation des SI
AFNOR S95N N 793	étude sur l'identification du patient

La liste de ces études n'est pas exhaustive, d'autres études seront intégrées dans ce document lors d'une prochaine édition.

2.2.6 La méthode MEHARI du CLUSIF

La méthode d'analyse de risques MEHARI™ (**ME**thode **H**armonisée d'**A**nalyse de **RI**sques), conçue par le CLUSIF, a été élaborée à partir des méthodes MARION et MELISA.
La base de connaissance utilisée est adaptable, évolutive et ouverte vers les risques opérationnels et métiers.

MEHARI™ s'adresse :
au management,
au risk-manager,
aux opérationnels,
aux auditeurs.

La méthode et la base de connaissance ont été traduites en anglais. De nombreuses structures publiques et privées, non seulement en France mais aussi en Belgique, au Canada, Luxembourg et Suisse, l'ont déjà mise en œuvre pour élaborer leur stratégie de sécurité.
L'ensemble est compatible avec les normes :
ISO 13335 pour la méthode,
ISO 17799:2000 et BS7799-2:2002 pour la base de connaissance.

Elle est susceptible d'être adaptée aux besoins spécifiques des établissements de santé.

La méthode permet de mettre en oeuvre une politique globale de sécurité structurée par :
Un plan stratégique,
Un (des) plan(s) opérationnel(s),
La constitution de tableaux de bord.

MEHARI™ repose sur une logique du risque afin d'en mesurer sa gravité :
Les causes d'un sinistre, ou la potentialité de survenance,
Les conséquences, ou l'impact,
Les scénarios de sinistres ainsi obtenus couvrent notamment les domaines métiers et techniques.

Pour l'accompagner, le logiciel Risicare propose un certain nombre de fonctionnalités comme l'audit des vulnérabilités, la gestion des scénarios, la planification d'actions et la mesure de la gravité des risques.

2.3 Les implications de la loi du 4 mars 2002

La loi du 4 mars 2002 place le patient au coeur du système de soins.

Elle entraîne des conséquences sur la sécurité des SIS qui devraient être traitées dans des décrets à venir.

Les professionnels et établissements de santé doivent donner accès à l'ensemble des informations concernant la santé du demandeur mais la loi ne fixe pas de limites aux données consultables, seulement un cadre minimal.
Le problème posé est celui de la qualité des données consultables. Doit-on distinguer les informations relatives à des hypothèses, des informations probables, des informations vérifiées ?
Le problème posé est aussi celui de leur contexte. Des données exactes, sorties de leur contexte, sont-elles représentatives de l'état de santé du patient et des soins qu'il reçoit ?

Aujourd'hui, il n'y a pas encore de réponse claire à ces questions.

L'accès direct aux informations sous-entend que les informations transmises sont toujours exactes et cohérentes puisque le patient n'a pas la capacité à détecter les erreurs ou les incohérences.
Comment peut-on, sans faire appel à un praticien, vérifier la qualité des données transmises ?
Quelle responsabilité est engagée en cas d'erreur dans la transmission de données médicales au patient (dossier incomplet, corrompu, transmission interrompue, impression partielle, ...) ?

Là encore, le législateur ne s'est pas encore prononcé, des décrets doivent clarifier ces notions.

Le texte précise que, lorsque la personne est prise en charge par une équipe de soins dans un établissement de santé, les informations la concernant sont réputées confiées par le malade (sauf opposition de sa part) à l'ensemble de l'équipe.
Cela sous-entend un accès complet et fiable aux données médicales personnelles par tous les personnels de l'équipe soignante suivant une politique d'autorisation établie.
Donc la saisie des données médicales doit être fiable et complète, faite sans délai par rapport à leur communication initiale.

L'utilisation de la carte professionnelle de santé peut-être rendue obligatoire dans un certain nombre de cas. Les décrets sur ce sujet ne sont pas encore parus.

Cela laisse supposer un procédé d'authentification des patients pour accéder à leurs données avec la problématique suivante :

- dans quelles conditions cet accès est-il envisagé ?
- quel type de procédé d'authentification sera-t-il utilisé ?

Cela laisse également supposer que l'exercice du droit du patient à traiter ses propres données doit être assorti d'un dispositif adapté.

Les données de santé à caractère personnel peuvent être entreposées chez un hébergeur. La loi ne définit pas encore ce qu'est un hébergeur, les décrets d'application doivent sortir prochainement.

2.4 Les implications de la nouvelle loi de transposition

Un projet de loi actuellement en cours d'examen par le Parlement français va modifier les dispositions de la loi Informatique et Libertés, en vue notamment de transposer en droit français les dispositions de la directive européenne n° 95/46/CE relative aux données personnelles.

Une des principales modifications apportée par le projet au régime actuellement en vigueur concerne le statut des données relatives à la santé : conformément à la directive, ces données sont considérées comme sensibles. Les données sensibles ne peuvent pas être traitées sans le consentement exprès de la personne concernée.

Ce principe est toutefois assorti de nombreuses exceptions en matière médicale. La finalité du traitement permet de déroger à l'interdiction de principe dans de nombreuses hypothèses qui couvrent a priori tous les cas de traitements de données par les professionnels de la santé : données traitées à des fins de traitement médical, de gestion des services de santé, dans le domaine de la recherche, traitements justifiés par l'intérêt public (ex. : sécurité sociale).

De plus le projet de loi de transposition prévoit que dans certains cas, le consentement de la personne ne sera pas suffisant pour autoriser la transmission des données nominatives.
Une loi à venir sera nécessaire pour préciser cet aspect de la question.

Ainsi, concrètement, les pratiques actuelles ne devraient pas être modifiées par l'entrée en vigueur de la future loi.

Un autre apport attendu du projet de loi est le renforcement des pouvoirs de la CNIL.

3 Liste des textes, références et documents applicables

Référence	Objet	Fiche de lecture
Référentiels, normes et recommandations techniques		
Norme CEN ENV 12924	norme européenne encadrant la sécurité des systèmes d'information de santé	22
Si51PSC1,2,3	politique de sécurité cadre pour les systèmes d'information	36
Si51PAU1,2	politique d'autorisation	31
Si51GAE	guide d'auto-évaluation des SI	29
Norme CEN ENV 12251	authentification et mot de passe pour les systèmes d'information de santé	40
Norme CEN ENV 13606	norme européenne encadrant le dossier du patient	en cours de rédaction
Norme CEN ENV 13608	norme européenne encadrant la sécurité des communications des systèmes d'information de santé	en cours de rédaction
Norme ISO 15408	critères communs pour l'évaluation de la sécurité des systèmes d'information. texte général à la SSI qui peut s'appliquer également à la santé.	en projet
Norme ISO 13335	management information communication technology security texte général à la SSI qui peut s'appliquer également à la santé.	en projet
Protection des données personnelles		
loi n° 78-17 du 6 janvier 1978	loi Informatique et Libertés	80
Délibération n° 97-008 du 4 février 1997 de la CNIL	portant adoption d'une recommandation sur le traitement des données de santé à caractère personnel	47
95/46/CE du 23 novembre 1995	protection des données personnelles et libre circulation de celle-ci	80
AFNOR S95N N 793	identification du patient	56
Code pénal : articles 226-16 à 24	relatif aux traitements des données personnelles	42

Référence	Objet	Fiche de lecture
décret 2002-637 du 29 avril 2002,	décret relatif à l'accès aux informations personnelles détenues par les professionnels et les établissements de santé en application des articles L. 1111-7 et L. 1112-1 du code de la santé publique	en projet
Projet de loi pour la protection des personnes physiques à l'égard des traitements de données à caractère personnel	Ce projet de loi, dit "de transposition", vise à modifier la loi 78-17 pour l'adapter en cohérence avec la directive Européenne.	en projet
Fiche thématique de la CNIL pour les professions de santé.	Recommandations de la CNIL pour le traitement des données de santé par les professionnels de santé.	en projet

Certification et contrôle		
Décret n° 2002-535 du 18 avril 2002,	décret relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information	65
ECF	Evaluation et Certification Française texte général à la SSI qui peut s'appliquer également à la santé.	68
Code de la santé publique : article L6113	obligation de la démarche d'accréditation des établissements de santé obligation de moyens	en projet
Recommandations de l'ANAES	critères GSI pour les établissements de santé	en projet
Protection contre la fraude		
loi n°88-19 du 5/01/88 modifiée par la loi 92-685 du 22/07/92 articles 323-1 à 323-7 du Code pénal)	loi relative à la fraude informatique texte général à la SSI qui peut s'appliquer également à la santé.	73
Confidentialité et secret professionnel		
Code pénal : articles 226-13,226-14, 226-15 et 432-9	Secret professionnel et secret des correspondances par voie de télécoms	77
Recommandation R (97) 5 du 13 février 1997 du Conseil de l'Europe	relative à la protection des données médicales (http://www.coe.fr/dataprotection/rec/r(97)5f.htm)	en cours de rédaction
Code de la santé publique : articles L1110 à L1112	le secret médical le droit à l'information du patient l'hébergement des données médicales	en projet
Textes généraux		
loi 2002-303 du 4 mars 2002 et code de la santé publique	loi "Kouchner"	80
décret 95-1000 du 6/09/95 modifié par le décret 97-503 du 21/05/97	le code de déontologie médicale	en projet
Code de la santé publique : articles L1112	l'hébergement des données médicales	en projet
Convention sur la cybercriminalité du 23/11/2001	Texte définissant les principes de la lutte contre la cybercriminalité et le besoin de protéger les intérêts légitimes liés au développement des technologies de l'information	en projet
Article 13 du Projet de loi relatif à la politique de santé publique	Modification du code de la santé publique et de la sécurité sociale pour encadrer le traitement de données de santé à des fins de recherches ou statistiques.	en projet

Annexe 1 : Recueil des fiches de lectures validées par le GT

A.1.1 Référentiels, normes et recommandations techniques

Fiche de lecture

Désignation du texte	Catégorisation et protection des systèmes d'information de santé		
Réf du texte	XP ENV 12924	Date du texte	Avril 2000
Auteur(s) / Origine	AFNOR		
Zone géo. concernée	Europe		
Population, structures et organismes concernés	Etablissements de santé		
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	2000

Objet, périmètre et limites du texte

Ce texte est une prénorme Européenne en cours de révision. Il fait référence à la recommandation européenne ITSEC et à la norme ISO 15408. Bien que ne faisant pas référence à l'aspect certification (exigences d'assurance de la norme ISO 15408), il en adopte néanmoins le concept de profils de protection.

Dédié aux systèmes d'information de santé, il permet de mettre en œuvre des profils de protection. Il traite de la sécurité des informations médicales, mais aussi de données de gestion administrative concourrant au soin des patients.

Ce texte est le seul actuellement en vigueur traitant spécifiquement des systèmes d'information des établissements de santé au niveau européen.

> " La Prénorme européenne spécifie un modèle et une méthode de catégorisation des systèmes d'informations de santé automatisés dans le contexte de la sécurité et du respect de la vie privée. La sécurité représente la préservation d'un niveau acceptable de **disponibilité**, de **confidentialité** et **d'intégrité** des données. Pour chaque catégorie spécifiée de systèmes, une série correspondante d'exigences et de recommandations de protection appropriée au niveau de risques inhérents à cette catégorie, est fournie. "

> " La Prénorme européenne s'applique à tous les systèmes d'information automatisés qui traitent des données de santé. Ceci inclut les systèmes qui participent directement aux soins des patients, par exemple les comptes rendus d'examens de laboratoires, mais également les systèmes statistiques ainsi que les systèmes administratifs qui fournissent un service opérationnel aux établissements de santé eux-mêmes, par exemple, les systèmes de prise en charge de la paie des employés, du personnel, de la planification et des questions financières. "

La Prénorme européenne s'applique à tous les objets du système d'information (données, individus, machines, programmes, ...)

Synthèse du texte

Modèle de catégorisation de sécurité

Le graphe ci-après détaille l'enchaînement déductif (extrait de la norme AFNOR) qui conduit de l'environnement aux recommandations de sécurité.

1 - Analyse des risques

↓

2 - Elaboration de la politique de sécurité

↓

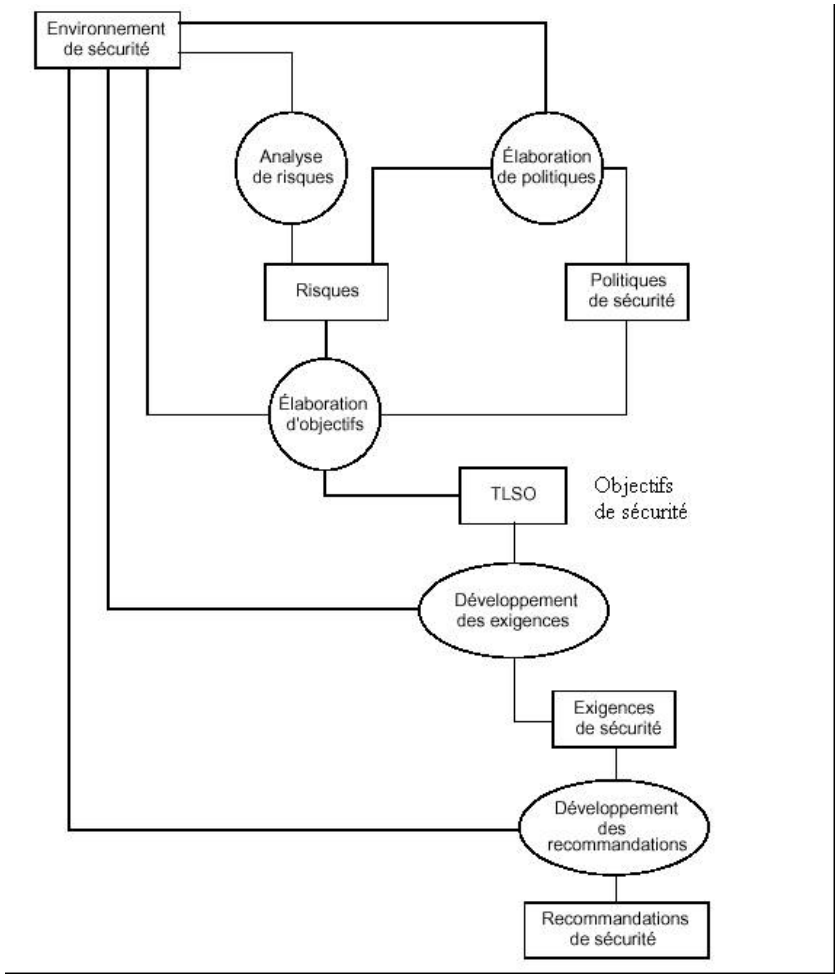
3 - Elaboration des objectifs

↓

4 - Définition des exigences de sécurité

↓

5 - Recommandations de sécurité



Le modèle décrit dans la norme définit la notion de profil. Un profil associe à chaque objet du système d'information la catégorie à laquelle il appartient et les exigences de sécurité sur cet objet.

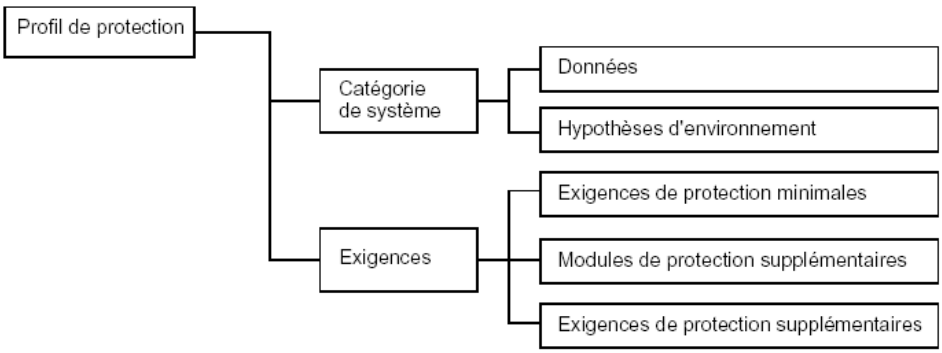
Il existe 6 catégories notées de 1 à 6, la catégorie 6 concerne les objets les plus sensibles.

- Catégorie I :
Disponibilité non critique, confidentialité sensible et intégrité non critique
- **Catégorie II :**
Disponibilité non critique, confidentialité sensible et intégrité critique
- Catégorie III :
Disponibilité critique, confidentialité sensible et intégrité critique
- Catégorie IV :
Disponibilité non critique, confidentialité très sensible et intégrité non critique
- Catégorie V :
Disponibilité non critique, confidentialité très sensible et intégrité critique
- **Catégorie VI :**
Disponibilité critique, confidentialité très sensible et intégrité critique

Il est défini 3 niveaux d'exigences :

- **exigences de référence**. Ce sont les exigences que tout HCIS[1] doit satisfaire quand il manipule des données autres que les données sensibles ;
- **exigences supplémentaires**. Ce sont les exigences que doivent satisfaire, en plus des exigences de référence, tous les HCIS qui traitent des données personnelles identifiables ;
- **exigences dépendant de l'environnement**. Elles doivent être satisfaites, en plus des exigences de référence et des exigences supplémentaires, par tous les HCIS ayant certaines caractéristiques relatives à l'utilisateur et à l'environnement.

Structure des profils de protection :



La méthodologie de catégorisation s'appuie sur un questionnaire relatif à chaque objet du système d'information.
Un arbre de décision (fourni par la norme) permet de déterminer, en fonction des réponses, la catégorie à laquelle appartient l'objet.

[1] HCIS : HealthCare Information Systems (Système d'information de santé)

L'environnement est pris en compte dans la formulation des "hypothèses". Les hypothèses correspondent à la description d'environnements types. Les hypothèses associées à la catégorie permettent ensuite de définir les exigences.

Il est défini :

6 hypothèses pour l'environnement physique,
3 hypothèses relatives à la connectivité physique
3 hypothèses relatives à la connectivité logique

Exigences / Profils de protection

Pour chaque profil de protection type (catégorie, environnement) la norme exprime des exigences.
Les exigences exprimées sont classées par domaine :

les exigences relatives au système
- identification
- contrôle d'accès
- responsabilité et audit
- précision
- fiabilité
- réseau et échange de données

les exigences relatives à l'administration
- gestion de la sécurité
- contrôle de la sécurité
- planification des actions
- protection contre les virus
- maintenance
- supports magnétiques et documentation

développement de logiciel

les exigences relatives au personnel
- recrutement
- gestion
- sensibilisation
- fin de contrat

respect de la vie privée

- les exigences physiques
  - contrôle des accès
  - protection contre le vol
  - exploitation - sauvegarde
  - incendie
  - dégât des eaux
  - catastrophes naturelles

Commentaires

Les principaux intérêts de ce texte résident dans :

- Sa conception :
  - Le groupe de travail à l'origine de ce texte est composé de professionnels de santé.

- Un référentiel pour l'accréditation :
  - Le programme d'accréditation des établissements de soins spécifie la prise en compte de la sécurité des systèmes d'information (GSI). Ce texte spécifie un ensemble d'exigences pour la mise en oeuvre de la sécurité dans les établissements de santé.
- Adaptabilité :
  - Classifier en sous-systèmes le système d'information du HCE, permet de déterminer l'ensemble des exigences spécifiques à ce sous-système. Dans le cas d'évolution d'un sous-système ou de changement de son environnement, il devient aisé d'y intégrer la réflexion sur l'impact du niveau de sécurité par un raffinement des exigences associées.

- La normalisation :
  - La définition d'un référentiel normalisé pour les établissements de santé européens (si la norme est adoptée définitivement) permettra de disposer d'une base commune à tous les acteurs pour évaluer la sécurité des SIS, et comparer les offres des SSII offrant leurs services dans ce domaine.
  - Elle permettra également d'homogénéiser le niveau de sécurité des SIS européens en fixant un objectif commun à tous les établissements.

- La notion de profils :
  - La catégorisation correspond à la définition des profils pour lesquels les exigences de sécurité sont formulées..

Cependant, on peut regretter que les points suivants, pourtant importants, ne soient pas ou insuffisamment, traités :

La catégorisation ne prend pas en compte les données non sensibles.

La traçabilité n'est pas un critère défini au même titre que les critères Disponibilité Intégrité Confidentialité.

Les notions de sous-système étendu et de sous-système restreint ne sont pas définies. Elles permettraient d'impacter les fonctions de sécurité de manière plus fine ayant ainsi un impact budgétaire optimisé.

Le sous-système étendu peut-être défini comme étant l'ensemble des objets d'un sous-système permettant de transmettre les informations du sous-système. Le sous-système étendu sera étudié vis à vis de la confidentialité.

Le sous-système restreint est l'ensemble des objets indispensable au fonctionnement minimal du sous-système. Le sous-système restreint sera étudié vis à vis de la disponibilité.

Il n'y a pas de prise en compte des aspects légaux dans la détermination des critères DIC, ou de certaines exigences (loi du 4 mars 2002).

L'ENV 12924 pourra être complétée par l'EBIOS ou certaines recommandations de la DCSSI :

- N°650/DISSI/SCSSI: Menace et attaques informatiques.
- N° 901/DISSI/SCSSI du 2 mars 1994 : Recommandation pour la protection des systèmes d'information.
- N° 150 SGDN / DISSI / SCSSI du 10 février 1991 : Fiche d'expression des objectifs de sécurité.
- N° 600/DISSI/SCSSI de Mars 1993 : Recommandation pour les postes de travail informatique.

La politique de sécurité n'est pas traitée explicitement. On peut compléter ce texte par les recommandations du GMSIH.

Les NTIC ne sont pas suffisamment prises en compte, en particulier l'ouverture des systèmes et l'interopérabilité des SIS et des SIH n'est pas suffisamment traitée.

Commentaires

Le déroulement type d'une étude selon la norme XP ENV 12924 peut être schématisé de la façon suivante :

- Etude du contexte.
- Découpage en sous-systèmes.
- Définition des sous-systèmes (approche ISO).
- Etude des besoins de sécurité.
- Sélection des éléments sensibles à étudier dans le cadre de la politique de sécurité.
- Etude des risques et identification des objectifs de sécurité.
- Catégorisation des objets.
- Définition des profils de protection.
- Définition des exigences pour chaque objet du HCIS.
- Évaluation de la sécurité.
- Inspection de chaque objet sensible du HCIS et contrôle des exigences de sécurité.
- Recommandations.
- Etude de l'écart entre les profils de protection et la situation observée.
- Regroupement et globalisation des concepts de sécurité à mettre en œuvre.

Fiche de lecture

Désignation du texte	Etude Politique de Sécurité des Systèmes d'Information des Etablissements de santé – Guide d'auto-évaluation de la sécurité des systèmes d'information			
Réf du texte	Si51GAE	Date du texte	31 mars 2003	
Auteur(s) / Origine	Groupement pour la Modernisation du Système d'information Hospitalier			
Zone géo. concernée	France et territoires d'outre mer			
Population, structures et organismes concernés	Etablissements publics et privés de santé			
Mise en oeuvre du texte	applicable ☒ appliqué ☐	date de mise en application	N/A	

Objet, périmètre et limites du texte

Définition
L'auto-évaluation consiste, pour les établissements de santé, à situer leur niveau de sécurité par rapport au niveau moyen de la PSC-SI et par rapport à leur risques spécifiques.
Le guide d'auto-évaluation est constitué d'un support logiciel et d'un manuel d'utilisation permettant de guider chaque établissement de santé dans son évaluation et dans la construction de son plan d'action pluriannuel de sécurité.

Objectifs
Les objectifs majeurs du guide d'auto-évaluation sont de permettre à chaque établissement de santé :

- D'apprécier son niveau de maturité en terme de sécurité de l'information par rapport aux principes de la Politique de Sécurité Cadre ;
- D'identifier son niveau de risque en fonction de cette maturité et des menaces pesant sur le système d'information ;
- D'identifier les actions prioritaires à conduire afin de réduire les risques ainsi identifiés ;
- De construire un plan d'action pluriannuel de mise en œuvre de la politique sécurité.

Synthèse du texte

Le Guide d'Auto-évaluation fait référence à la PSC-SI qui permet d'étalonner un certain niveau de sécurité. Ainsi, dans chaque domaine identifié de cette PSC-SI, les principes fondamentaux seront mis en exergue et un jeu de questions-réponses est proposé.
En fonction des réponses de l'établissement, et d'une pondération dite « de risque », le guide affecte un coefficient de sécurité qui révèle par consolidation, le niveau de maturité domaine par domaine.
Afin de permettre à tout établissement de santé de mener son auto-évaluation, le support assure une visualisation rapide et présentable des résultats obtenus (traitement et dépouillement des réponses et présentation des résultats sous forme de graphiques), une simplicité d'utilisation (sur excel), et une transparence des traitements (calculs automatisés).

L'aide à la réalisation du plan d'action pour les établissements repose sur :

- Un classement des principes de sécurité à mettre en œuvre par ordre prioritaire, réalisé par l'outil logiciel; les priorités sont basées sur la contribution de chaque principe à la réduction des risques de l'établissement,

- Un récapitulatif de l'enchaînement recommandé pour la mise en œuvre des principes de la PSC-SI,
- *Une aide à la décision pour la construction du plan d'action pluriannuel, tenant compte d'une part des priorités proposées par l'outil logiciel, d'autre part du coût et de la faisabilité (technique, organisationnelle) estimés par l'établissement.*

Fiche de lecture

Désignation du texte	Etude Politique de Sécurité des Systèmes d'Information des Etablissements de santé – Politique d'autorisation		
Réf du texte	Si51PAU1,2	Date du texte	31 mars 2003
Auteur(s) / Origine	Groupement pour la Modernisation du Système d'information Hospitalier		
Zone géo. concernée	France et territoires d'outre mer		
Population, structures et organismes concernés	Etablissements publics et privés de santé		
Mise en oeuvre du texte	applicable ☒ appliqué ☐	date de mise en application	N/A

Objet, périmètre et limites du texte

Définitions

Politique d'Autorisation

Une autorisation est « l'attribution de droits, comprenant la permission d'accès sur la base de droits d'accès » (source : ISO 7498-2, traduction AFNOR).

Déclinaison de la politique de sécurité des systèmes d'information, la Politique d'Autorisation est le « document cadre » de la gestion du contrôle d'accès logique d'un établissement.

La Politique d'Autorisation, établie dans le cadre de la présente étude, définit en particulier :

- La modélisation fonctionnelle des autorisations (lien entre un utilisateur, son rôle et ses droits sur une ressource donnée en fonction d'un contexte) ;
- Les règles de gestion des autorisations et de traçabilité des accès ;
- Les modalités d'administration des autorisations (attribution, révocation, délégation…).

Habilitation

L'habilitation est « le droit accordé à un individu d'accéder à des informations dont le niveau de sécurité est inférieur ou égal à un niveau déterminé » (ISO/IEC IS 2382-8 (1998), AFNOR. Commission de Normalisation Informations de Santé).

La Politique d'Autorisation s'appuie, pour autoriser l'accès à des ressources, sur les habilitations.

Objectifs

L'objectif de l'étude est de proposer une modélisation fonctionnelle et organisationnelle des autorisations au sein des systèmes d'information des établissements de santé, afin de pouvoir garantir :

- La qualité et de la pérennité de la sécurité d'accès au système d'information, par une définition homogène de rôles par métier et l'attribution d'autorisations aux personnes via ces rôles ;
- L'imputabilité des opérations à leurs auteurs via l'attribution d'autorisations à des personnes nommément identifiées dans le système d'information ;
- L'harmonisation de la gestion des autorisations pour toutes les activités de l'établissement ;
- La rigueur dans l'attribution et la révocation des autorisations ;
- Une meilleure protection des accès lors de l'ouverture du SIH sur d'autres SI,

grâce à la réflexion menée en amont dans le cadre de la politique d'autorisation de l'établissement.

Synthèse du texte

Modélisation fonctionnelle des autorisations

Le modèle proposé dans cette politique d'autorisation est une adaptation et une extension des principes du modèle RBAC (Role Based Access Control) adaptés pour tenir compte des contraintes liées au contexte et au temps. Les autorisations sont en effet déterminées dynamiquement pour répondre aux besoins propres aux systèmes d'information des établissements de santé.
La notion de rôle est fondamentale pour le modèle d'autorisation présenté. Toutefois, le contrôle d'accès d'un système d'information nécessite aussi de faire appel aux notions suivantes :

- Contenu sémantique du dossier médical : tout le contenu du dossier ne doit pas être accessible à tous les professionnels de santé (PS). En effet, certaines informations (anatomie pathologique, virologie…) sont particulièrement confidentielles. D'autre part, un membre du personnel soigné au sein de son propre établissement de santé peut demander que son dossier reste confidentiel ;
- Structure d'affectation : un PS est affecté à une unité fonctionnelle, et ne doit accéder qu'aux informations nécessaires à l'exercice des soins propres à son UF (ex : laboratoire, anesthésie, pharmacie…) ;
- Mode et lieu d'accès : il est souhaitable que certaines informations puissent n'être accessibles qu'à partir de certains emplacements uniquement. Cette notion permet par exemple de traiter le contrôle d'accès aussi bien via un portail de santé (localisation externe à l'établissement de santé) que dans un service d'urgence (localisation interne à l'établissement de santé).
- Temps : les droits d'accès sont généralement restreints à une fenêtre temporelle liée à la présence du patient dans le service ou à une prise de rendez-vous ;
- Restriction d'accès à certains dossiers : dans certains cas, un PS ne doit accéder qu'aux dossiers des patients dont il a ou a eu personnellement la charge. C'est le cas notamment des patients VIP ou des membres du personnel de l'établissement. La relation entre un praticien et ses patients est donc un des critères qui doit pouvoir être utilisé pour le contrôle d'accès ;
- A la demande du patient, opposition faite à certains PS d'accéder à son dossier : la loi du 4 mars 2002 permet au patient d'interdire à certains PS d'accéder à son dossier patient ;
- Autorisation d'accès accordé par le patient à des PS externes à l'établissement : un patient est susceptible d'indiquer quels sont les praticiens externes à l'établissement auxquels il souhaite donner accès à son propre dossier (médecin traitant par exemple).

D'autre part, le modèle présenté permet aussi de tenir compte des contraintes de coopération, la capacité à traiter un patient primant sur les autres considérations. La délégation de pouvoirs doit donc être possible au sein des équipes, voire en dehors des équipes dans certaines conditions (gardes, urgence…). Des exceptions au contrôle d'accès seront prévues, avec des contraintes de traçabilité et de justifications adéquates pour éviter les abus.

Afin de répondre au besoin de mise en œuvre progressive, le modèle cible est accessible en trois étapes :

- **Etape 1 : Modèle simple**

Le modèle simple est basé sur l'attribution de droits d'accès par « métier ». Chaque utilisateur, identifié et authentifié de façon unique, se verra attribuer un rôle basé sur des autorisations propres à son métier pour l'accès aux ressources c'est à dire notamment aux éléments du dossier du patient. On

pourra identifier ainsi le rôle de « l'infirmière », le rôle du « médecin », le rôle du « biologiste »…

- **Etape 2 : Modèle intermédiaire**

Le modèle intermédiaire complète le modèle simple par la notion « d'affectation » de l'utilisateur à une structure (une organisation de santé, un service…). Cette notion permet de restreindre l'accès au dossier des patients d'une structure, d'un service pour un professionnel affecté à cette structure.

Ce modèle intègre aussi la notion de « patient acteur » : ce dernier peut s'opposer à l'accès d'un professionnel particulier aux éléments de son dossier conformément à la loi du 4 mars.

- **Etape 3 : Modèle complet (cible)**

Le modèle complet complète le modèle intermédiaire en ajoutant les éléments nécessaires au suivi de la « trajectoire du patient » .

La notion de « trajectoire du patient » a pour vocation de permettre, pour certains PS, la restriction de l'accès au dossier patient à certaines périodes temporelles.

Ces périodes sont déterminées sur la base d'évènements survenant lors de la prise en charge du patient. Chaque événement est caractérisé par une date de début et une date de fin.

Cette trajectoire est à considérer dans son acception la plus large. Les événements sont de différents types : les périodes d'hospitalisation (qui ont une certaine durée), les actes réalisés suite à une demande de prestation (consultations, analyses, actes d'imagerie, etc. qui sont ponctuels). La présence physique du patient n'est pas forcément constatée aux différentes étapes de cette trajectoire : la délivrance de médicaments à la pharmacie correspond à une demande de prestation, et donne droit au pharmacien d'accéder à certains éléments du dossier patient, bien que celui-ci ne soit pas physiquement présent.

Ces événements peuvent aussi être déclenchés sans que le patient soit en cours de traitement dans l'établissement. Ce sera le cas par exemple du suivi des dossiers patients dans un traitement de cancérologie.

Afin de faciliter l'utilisation des modèles et de dégager les règles générales de sécurité concernant la gestion du contrôle d'accès logique, cinq scénarios sont détaillés :

- Ouverture de session ;
- Accès à une ressource ;
- Modification des rôles activés ;
- Clôture de session ;
- Accès à une ressource par exception au contrôle d'accès.

Modalités d'administration des autorisations

Dans un établissement de grande taille, le nombre de rôles et d'utilisateurs sera très important, et génèrera par conséquent une lourde charge d'administration. L'organisation fréquemment adoptée est de créer une équipe dédiée à la gestion des autorisations. Toutefois, ce principe permet rarement d'obtenir une réactivité suffisante compte tenu du fonctionnement d'un établissement de santé, dans lequel certaines catégories d'utilisateurs changent fréquemment d'affectation ; de nombreuses exceptions sont susceptibles d'être demandées.

Il est donc recommandé d'adopter une organisation décentralisée pour l'administration des droits d'accès.

L'administration des droits d'accès repose sur plusieurs éléments :

- Description de l'organisation de l'établissement en éléments de structure ;
- Définition des rôles et de leur hiérarchie ;
- Attribution d'autorisations aux rôles ;
- Affectation d'un utilisateur dans un élément de structure avec un rôle déterminé.

Les modèles d'autorisation proposés séparent explicitement le rôle d'un utilisateur (médecin, infirmier,

DIM, médecin chargé de la vigilance…) et l'élément de structure auquel cet utilisateur est affecté.
Grâce à cette séparation, la définition des rôles pourra être réalisée de manière centralisée par quelques responsables (DIM, responsables d'application…).
A contrario, l'affectation des utilisateurs à un élément de structure avec un certain rôle pourra être décentralisée, et gérée localement par les responsables concernés (ex : une surveillante pourra déclarer les affectations de ses infirmières).
Afin de faciliter l'utilisation des modèles et de dégager les règles générales de sécurité concernant l'administration des autorisations, cinq scénarios sont proposés :

- Création du compte d'un utilisateur interne ;
- Création du compte d'un intervenant externe ;
- Suppression d'un compte ;
- Définition des rôles ;
- Affectation d'un utilisateur à un élément de structure avec un rôle.

Différents modèles d'organisation sont proposés concernant l'administration des autorisations, de façon à prendre en compte les spécificités de l'établissement et de son système d'information :

- Concernant la **définition des rôles,** il est recommandé de procéder à une définition de rôles « standard » par le DIM, validés par le Collège d'information médicale et / ou la CME. De plus, pour prendre en compte les spécificités éventuelles d'un service, des rôles « spécifiques » peuvent être définis par le chef de service en collaboration avec le DIM. Ces rôles doivent néanmoins respecter la politique d'autorisation de l'établissement et être validés en instance.
- Concernant **l'attribution des rôles** aux utilisateurs, trois modèles d'organisation sont *envisageables :*
  - Une organisation centralisée où la gestion des ressources humaines[2] effectue à la fois l'affectation de l'utilisateur à un élément de structure et l'attribution des rôles. Dans ce cas, un système de calcul et d'attribution automatique des droits est vivement conseillé ;
  - Une organisation semi-décentralisée où l'affectation des utilisateurs reste sous la responsabilité de la gestion des ressources humaines, et l'attribution des rôles est dévolue au management de proximité (responsables d'encadrement, cadres supérieurs…) ;
  - Une organisation décentralisée où à la fois l'affectation des utilisateurs et l'attribution des rôles sont réalisés par le management local.
- Concernant **la supervision et le contrôle** de l'administration des droits d'accès : le suivi permanent relève de la co-responsabilité du DIM et du RSSI. Il est de plus recommandé que ces derniers élaborent un rapport annuel de synthèse comprenant un bilan des droits existants, les évolutions apportées, un suivi qualité et l'analyse des incidents observés.

Démarche de mise en œuvre de la politique d'autorisation

Tous les établissements de santé ont d'ores et déjà abordé le sujet de la mise en œuvre des autorisations au travers des habilitations définies pour l'utilisation d'une ou plusieurs applications de SIH.

L'objectif d'une politique d'autorisation est une harmonisation des pratiques de gestion et d'administration du contrôle d'accès logique pour l'ensemble des applications du SIH.

La démarche de mise en œuvre d'une politique d'autorisation doit s'appuyer sur un projet porteur : la mise en place d'une application de production de soins, d'un projet d'infrastructure (annuaire et single sign on…).

[2] Au sein d'un établissement de santé, différentes entités sont impliquées dans la gestion des ressources humaines : la DRH, la direction ou le bureau des affaires médicales, la direction des soins infirmiers.

Le choix d'un modèle fonctionnel parmi ceux proposés (simple, intermédiaire, complet) dépend de la nature et de la maturité du système d'information de l'établissement et des évolutions envisagées (ouverture du SIH vers l'extérieur…).

Une étape importante est la définition des référentiels qui seront manipulés par le modèle d'autorisation : les structures d'affectation, la classification des ressources, la nomenclature des rôles « métier ».

La définition des règles de gestion du contrôle d'accès logique, de traçabilité et d'administration aident l'établissement pour la définition des rôles.

L'attribution des rôles aux utilisateurs doit être accompagnée d'actions de sensibilisation et de communication.

Fiche de lecture

Désignation du texte	Etude Politique de Sécurité des Systèmes d'Information des Etablissements de santé – Politique de Sécurité Cadre pour les Systèmes d'Information (PSC-SI)		
Réf du texte	Si51PSC1,2,3	Date du texte	31 mars 2003
Auteur(s) / Origine	Groupement pour la Modernisation du Système d'information Hospitalier		
Zone géo. concernée	France et territoires d'outre mer		
Population, structures et organismes concernés	Etablissements publics et privés de santé		
Mise en oeuvre du texte	applicable ☒ appliqué ☐	date de mise en application	N/A

Objet, périmètre et limites du texte

Définition et périmètre de la PSC-SI

La Politique de Sécurité Cadre des Systèmes d'Information est l'ensemble des principes juridiques, humains, organisationnels et techniques qu'il est recommandé de mettre en œuvre pour créer, gérer, protéger le système d'information, en particulier les informations sensibles, au sein de l'établissement de santé et lors de ses échanges avec les autres systèmes d'information de santé (autre établissement de santé, réseau de santé, médecin correspondant, patient)

Le périmètre de la PSC-SI concerne :
La définition des principes de sécurité à mettre en œuvre pour les applications et données du système d'information d'un établissement de santé ;
Les conditions d'utilisation de dispositifs de sécurité par le personnel de l'établissement de santé et par les usagers externes en relation avec l'établissement (patient, professionnel de santé, …), ainsi que les services de support et d'accompagnement nécessaires (formation, sensibilisation, hot lines, …) ;
La mesure de l'efficacité des dispositifs de sécurité et leur mise à jour.

Objectifs de la PSC-SI

La PSC-SI a pour objectifs :

De constituer un cadre de référence pour la sécurité des systèmes d'information hospitaliers et de leurs relations avec d'autres systèmes d'information de santé. Ce cadre de référence peut être également utilisé par les établissements pour élaborer leurs cahiers des charges à destination des fournisseurs ;
De constituer une aide pragmatique à l'élaboration de la politique de sécurité propre à un établissement de santé : la démarche d'élaboration est guidée, les dispositifs et les niveaux de sécurité sont documentés.

La PSC-SI est composée de trois parties qui sont présentées ci après.

Synthèse du texte

PSC-SI Partie 1 : Fondements de la Politique de Sécurité

La première partie de la PSC-SI présente les fondements de la Politique de Sécurité : principales définitions, bases réglementaires et normatives, axes stratégiques de la politique de sécurité.

Les finalités de la Politique de Sécurité sont les suivantes :

- Sensibiliser aux risques qui menacent l'information et les systèmes d'information des établissements de santé, ainsi qu'aux moyens disponibles pour s'en prémunir ;
- Créer un cadre général, adapté aux systèmes d'information hospitaliers, pour aider les personnes chargées d'élaborer et de mettre en œuvre des mesures, des consignes, des procédures cohérentes, en vue d'assurer la sécurité de l'information et du système d'information automatisé ;
- Promouvoir la coopération entre les différents services et acteurs de l'établissement pour l'élaboration et la mise en œuvre de ces mesures, consignes et procédures ;
- Susciter la confiance des utilisateurs et des patients dans le système d'information automatisé.

Les principes et les règles de la PSC-SI s'appuient sur la déontologie des activités médicales, les lois et les réglementations, ainsi que dans les normes et recommandations émanant d'organisations du monde médical ou du secteur de la sécurité des systèmes d'information.

La Politique de sécurité porte également les valeurs fondamentales de sécurité dont l'appropriation par les concepteurs et utilisateurs des systèmes d'information de santé est fortement encouragée.

Ces valeurs constituent les axes stratégiques de la Politique de sécurité :

1. Favoriser le développement de la coopération entre professionnels de santé en instaurant un climat de confiance, grâce à la sécurité des systèmes d'information ;
2. Placer le patient au cœur de la politique de sécurité :
    - Rechercher en permanence un compromis acceptable entre impératifs d'efficacité du soin et impératifs de sécurité de l'information ;
    - Respecter le droit à la vie privée du patient, par la garantie de l'anonymat et à l'assurance de la confidentialité des informations médicales.
3. Etablir une politique de sécurité de l'établissement conforme aux bonnes pratiques, et la décliner pour les relations avec les partenaires de santé :
    - Classifier les ressources, dont les différentes parties du dossier de santé ;
    - Mettre en place une politique d'autorisation conforme à la législation et au besoin de protection des ressources.
4. Articuler la politique de sécurité de l'information avec la qualité et la gestion des risques :
    - Mesurer régulièrement la qualité de la sécurité de l'information ;
    - Intégrer dans le cadre des vigilances instaurées par l'établissement, la vigilance sur la sécurité du système d'information (alerte et processus de réaction).

PSC-SI Partie 2 : Principes et règles de mise en œuvre

La deuxième partie de la PSC-SI propose au responsable de l'élaboration de la Politique de Sécurité de l'établissement le choix parmi 39 principes déclinés en 168 règles.

Elle est articulée autour de 10 chapitres qui prennent en compte les préoccupations suivantes :

- Organisation et management de la sécurité du système d'information :
  - Chapitre 1.1 : Politique de sécurité
  - Chapitre 1.2 : Management de la sécurité
- Sécurité pour la maîtrise des risques :
  - Chapitre 2.1 : Inventaire et classification des ressources
  - Chapitre 2.2 : Sécurité et ressources humaines
  - Chapitre 2.3 : Sécurité physique et sécurité de l'environnement
  - Chapitre 2.4 : Exploitation informatique et gestion des réseaux
  - Chapitre 2.5 : Contrôle d'accès logique
  - Chapitre 2.6 : Développement et maintenance des applications et des systèmes
  - Chapitre 2.7 : Gestion de la continuité
  - Chapitre 2.8 : Respect de la réglementation interne et externe

Chaque chapitre comprend des principes de sécurité.

Chaque principe est documenté de la manière suivante :

- Intitulé du principe ;
- Objectif du principe ;
- Pré requis (principes de la PSC-SI à mettre en œuvre préalablement) ;
- Préalable à (principes de la PSC-SI dont le principe en cours est un pré requis).

Les pré requis et préalables sont utilisés pour établir le graphe d'ordonnancement des actions de sécurité dans le Guide d'Auto-évaluation.

Pour chaque principe, les règles sont présentées de la façon suivante :

- Intitulé de la règle ;
- Classement de la règle (voir définition ci-après) ;
- Description de la règle.

Les règles font l'objet d'un classement en trois niveaux :

Niveau 1 :

Niveau établi sur la base des pratiques de sécurité couramment constatées, permettant de parer aux urgences liées aux failles de sécurité. Il met également l'accent sur les aspects organisationnels et la continuité des services afin de préparer l'informatisation de la production de soins.

Niveau 2 :

En complément des règles de niveau 1, le niveau 2 correspond aux règles dont la mise en œuvre permet de se conformer à l'état de l'art pour atteindre un bon niveau de sécurité.

Niveau 3 :

Le niveau 3 correspond à des règles dont la mise en œuvre présente un intérêt réel mais qui sont néanmoins en avance sur l'état de l'art.

Ce classement permet ainsi une progressivité dans la mise en œuvre du plan d'action.
Les niveaux 1, 2 ou 3 se traduisent par un coefficient de contribution à l'efficacité de la politique de sécurité qui est pris en compte dans le calcul des priorités d'action du Guide d'Auto-évaluation.

La PSC-SI a été construite en conformité avec la norme ISO 17799.

PSC-SI Partie 3 : Guide de rédaction de la politique de sécurité des systèmes d'information de l'établissement

Cette partie indique la démarche à suivre par l'établissement pour rédiger sa propre politique en s'appuyant sur le contenu de la politique de sécurité cadre. Elle explicite les étapes et acteurs de ce projet, et indique les facteurs - clés de sa réussite.

Le rédacteur de la politique de sécurité des systèmes d'information de l'établissement est le RSSI (Responsable de la sécurité des systèmes d'information), il est mandaté par le directeur de l'établissement. Il s'appuie sur le comité de sécurité chargé de valider le contenu de la politique de sécurité (COSSI).

Le rédacteur procède en premier lieu à l'identification des fondements de la politique de sécurité, notamment les axes stratégiques et enjeux majeurs de sécurité pour l'établissement, en s'appuyant sur la partie 1 de la PSC-SI.

Il procède ensuite à l'auto-évaluation qui mettra en évidence les principes prioritaires à mettre en oeuvre. Il sélectionne ainsi les principes proposés dans la partie 2 de la PSC-SI et les soumet pour validation, au travers d'éventuelles réunions de travail thématiques, aux personnes compétentes de l'établissement (DIM, responsable juridique, informaticiens, représentants des utilisateurs et maîtres d'ouvrage des projets…).

Pour faciliter la communication de la politique de sécurité auprès de l'ensemble des personnels de l'établissement, il est conseillé de rédiger un document de synthèse qui insiste sur l'importance de la sécurité du système d'information en tant que dispositif permettant la création, le partage et la conservation de l'information.

Ce document présente de plus les responsabilités concernant la gestion de la sécurité du système d'information.

Les règles opérationnelles de sécurité doivent être définies en fonction du plan d'action sécurité qui comprend notamment les chartes de confidentialité, les chartes de sécurité des réseaux, les plans de continuité. Elles sont rédigées en collaboration avec les professionnels compétents sur le sujet (DIM, informaticiens, maîtrise d'ouvrage des projets de système d'information…) qui participent au comité opérationnel de sécurité.

Commentaires

Cette étude ne fait pas référence aux travaux européens (Prénorme ENV 12924 , 13606 et 13608) relatifs à la sécurité des systèmes d'information de santé.

Fiche de lecture

Désignation du texte	AUTHENTIFICATION		
Réf du texte	Norme CEN ENV 12251	Date du texte	1999
Auteur(s) / Origine	CEN TC 251		
Zone géo. concernée	Europe		
Population, structures et organismes concernés	Systèmes d'information de santé		
Mise en oeuvre du texte	applicable ☐ appliqué ☐	date de mise en application	

Objet, périmètre et limites du texte

Il s'agit de l'ensemble des dispositions indispensables à mettre en œuvre dans un SMSI (système de management de la sécurité de l'information) pour la gestion des mots de passe dans le monde médical.

Synthèse du texte

Le mot de passe doit :

contenir plus de 6 caractères
être stocké, crypté
être changé tous les deux mois.

Le système doit :

être déconnecté après 3 tentatives,
permettre le changement du mot de passe par l'utilisateur,
afficher la date et l'heure de la connexion précédente et toute connexion infructueuse après toute demande de connexion

Commentaires

Une bonne gestion des mots de passe constitue le pré requis indispensable d'une authentification dans une infrastructure à clés symétriques.
C'est par ailleurs le niveau le plus bas d'une authentification. Même dans des infrastructures à clés symétriques, il existe des niveaux d'authentifications supérieurs basés en particulier sur l'addition d'un élément physique (token, carte,…) à un élément logique (mot de passe, certificat, Pin Code)
Un travail sérieux sur l'authentification devrait traiter de l'authentification dans les infrastructures à clés asymétriques (PKI).

Cette norme est dépassée, elle n'aborde que le problème de la force du mot de passe et ne traite pas de l'organisation qui l'entoure ni de sa gestion.

De plus la force du mot de passe doit maintenant être renforcée à 8 caractères pour assurer une meilleure protection contre l'utilisation de moyens de calculs plus performants.

A.1.2 Protection des données personnelles

Fiche de lecture

Désignation du texte	Loi Informatique et Libertés - articles 226-16 à 226-24 du Code pénal		
Réf du texte	Loi n° 78-17	Date du texte	6 janvier 1978
Auteur(s) / Origine	Parlement		
Zone géo. concernée	France		
Population, structures et organismes concernés	Tout organisme, toutes personnes physiques ou morales		
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	Janvier 1978

Objet, périmètre et limites du texte

La loi Informatique et Libertés du 6 janvier 1978 encadre la collecte et le traitement des informations nominatives.
Cette loi pose le socle juridique commun, les principes fondamentaux en matière de protection des données personnelles. Elle ne réglemente pas spécifiquement le traitement des données personnelles dans le secteur médical.
Les articles 226-16 à 226-24 du Code Pénal éditent les sanctions pénales afférentes au non respect des prescriptions de la loi Informatique et Libertés.
L'objectif de cette réglementation est la protection de la vie privée des personnes concernées par le traitement.

Synthèse du texte

1. Notions de donnée nominative et de traitement

Une *donnée nominative* au sens de la législation, c'est toute donnée qui permet l'identification de la personne physique, même indirectement (article 4 de la loi). Sont par exemple considérés comme des données indirectement nominatives : un n° de matricule, de téléphone, une adresse de courrier électronique, le recoupement de plusieurs renseignements non nominatifs comme une pathologie rare et un code postal.

La notion de traitement automatisé d'informations nominatives est large (article 5 de la loi) :
Tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou base de données (interconnexions, rapprochement, consultations, communications d'informations nominatives).

2. La législation accorde un certain nombre de droits aux personnes dont les données sont collectées :

Principe d'interdiction du traitement des données dites sensibles sans le consentement exprès, c'est-à-dire écrit. Concerne les informations faisant apparaître, même indirectement les origines raciales, les opinions politiques, philosophiques, religieuses, les mœurs, l'appartenance syndicale (art 31). L'utilisation du répertoire national d'identification des personnes physiques nécessite une autorisation par décret en Conseil d'Etat (art 18). Dans l'hypothèse d'un traitement ayant pour fin la recherche dans le domaine de la santé, si la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en œuvre du traitement de données (art. 40-4).

Droit d'information (article 27 de la loi de 1978) : les personnes auprès desquelles sont recueillies les données nominatives doivent être informées : du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des personnes destinataires des informations, de l'existence d'un droit d'accès et de rectification.

Droit d'opposition : toute personne a le droit de s'opposer, pour des raisons légitimes, à ce que les informations nominatives la concernant fassent l'objet d'un traitement. Cette disposition ne s'applique pas aux traitements opérés par un établissement public ou une personne morale de droit privé gérant un service public. L' article 40-4 de la loi « informatique et libertés » prévoit également que toute personne a le droit de s'opposer à ce que des données nominatives la concernant fassent l'objet d'un traitement ayant pour fin la recherche dans le domaine de la santé

3. La législation prévoit qu'un traitement doit respecter un certain nombre de grands principes :

Principe de loyauté de la collecte des données : prohibition des collectes réalisées à l'insu des personnes concernées, par des moyens frauduleux.

Principe dit de finalité : les données sont collectées pour des finalités déterminées, elles ne peuvent pas être traitées ultérieurement pour d'autres finalités. Les données recueillies doivent être adéquates et pertinentes au regard de la finalité du traitement. Préciser la finalité d'un fichier est essentiel car c'est en fonction de cette finalité que sont déterminées les données qu'il est possible de collecter, la durée de conservation, les destinataires des données c'est-à-dire les personnes auxquelles les données sont communiquées.

Principe de mise à jour des données : un fichier doit être complété ou corrigé lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information contenue dans le fichier. Les modifications apportées aux traitements doivent être portées à la connaissance de la CNIL (art.19).

Droit à l'oubli : la conservation des données ne doit pas excéder ce qui est nécessaire à la finalité du traitement. Au-delà de cette durée, les informations nominatives ne peuvent être conservées qu'à des fins historiques, statistiques ou scientifiques.

Obligation de sécurité : toute personne ordonnant ou effectuant un traitement s'engage à prendre toutes les précautions utiles afin de préserver la sécurité des informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés (art. 29). Les mesures de sécurité tant physique que logique mises en œuvre doivent être adaptées à l'utilisation qui est faite de l'ordinateur, à sa configuration, à l'existence ou non d'une connexion à Internet... Obligation de ne communiquer les données qu'aux destinataires et tiers autorisés à en connaître. D'une façon générale, les données nominatives ne peuvent être communiquées qu'aux destinataires et tiers autorisés à en connaître en vertu de la loi.

4. Formalités préalables

Le choix de la formalité à accomplir dépend de la nature juridique de l'organisme responsable du traitement et du type de traitement concerné.
La loi prévoit que tout traitement informatique d'informations nominatives mis en œuvre par une personne privée doit faire l'objet d'une déclaration préalable, avant sa mise en service, auprès de la CNIL, Commission nationale de l'informatique et des libertés (art 16).

La déclaration du fichier n'exonère pas la personne de sa responsabilité de respecter les dispositions de la loi.
Les traitements mis en œuvre par les organismes du secteur public c'est à dire, les traitements opérés par l'Etat, un établissement public, une collectivité territoriale, une personne morale de droit privé gérant un service public (établissement de santé participant à l'exécution du service public hospitalier) sont décidés par arrêté ou décret pris après avis préalable de la CNIL (art. 15).

La déclaration ou la demande d'avis doivent notamment préciser : la finalité du traitement, le service auprès duquel s'exerce le droit d'accès, les caractéristiques de l'application, l'architecture des moyens techniques utilisés, les mesures relatives à la sécurité, les catégories d'informations traitées et leur durée de conservation, les destinataires des informations, les garanties relatives à l'information préalable et au droit d'accès.

La procédure de la déclaration est simplifiée, pour les traitements les plus courants et les moins dangereux (art. 17).

La procédure devient une demande d'autorisation pour les traitements de données de santé à des fins de recherche (chap V bis).
Sont ainsi concernés les projets de recherche médicale (épidémiologie, recherche biomédicale…) qui d'une part prévoient le recueil et la transmission d'informations médicales à un organisme de recherche privé ou public de données directement ou indirectement nominatives et d'autre part le recours à des moyens informatiques pour le traitement des données.

La procédure de la demande d'autorisation concerne les traitements de données de santé ayant pour fin l'évaluation des pratiques de soins et de prévention. Les données de santé indirectement nominatives (à l'exclusion de celles comportant le nom, le prénom du patient ou son numéro de sécurité sociale), qu'elles soient issues des fichiers des professionnels de santé, des systèmes d'information hospitaliers (PMSI), ou des fichiers des caisses de sécurité sociale (SIAM), peuvent être transmises et exploitées à des fins d'évaluation des pratiques de soins et de prévention (chap V ter)

5. Rôle de la CNIL

Elle est chargée de veiller au respect des dispositions de la loi Informatique et Libertés. Elle possède également un pouvoir de contrôle, et peut procéder à des missions de vérification sur place. Elle enregistre les demandes d'avis du secteur public, les déclarations du secteur privé et les autorisations, en tenant à jour et en mettant à la disposition du public le "fichier des fichiers", établit des normes simplifiées (pouvoir réglementaire), garantit le droit d'accès indirect, en particulier au fichier des Renseignements Généraux, instruit les plaintes, informe les personnes de leurs droits et obligations, conseille les personnes et organismes qui lui demandent, propose au gouvernement les mesures législatives ou réglementaires qui lui paraissent utiles.

6. Sanctions pénales
Le non-respect de la loi Informatique et Libertés est lourdement sanctionné pénalement :

l'omission de la déclaration préalable constitue le délit de création de fichier clandestin : trois ans d'emprisonnement et 45 000 euros d'amende (article 226-16 du Code pénal),

manquement à la sécurité, défini comme le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés : cinq ans d'emprisonnement et 300 000 euros d'amende (article 226-17 du Code pénal),

collecte frauduleuse, déloyale ou illicite : cinq ans d'emprisonnement et 300 000 euros d'amende (article 226-18 du Code pénal),

collecte d'informations sensibles hors les cas prévus par la loi : cinq ans d'emprisonnement et 300 000 euros d'amende (article 226-19 du Code pénal),

conservation des informations au-delà de la date prévue : cinq ans d'emprisonnement et 300 000 euros d'amende (article 226-20 du Code pénal),

délit de détournement de finalité d'informations nominatives : cinq ans d'emprisonnement et 300 000 euros d'amende (article 226-21 du Code pénal),

délit de divulgation illicite d'informations nominatives : fait de porter, sans autorisation de l'intéressé, des informations dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou a l'intimité de sa vie privée à la connaissance d'un tiers qui n'a pas qualité pour les recevoir : un an d'emprisonnement et 7 500 euros d'amende (article 226-22 du Code pénal),

la non-information des personnes interrogées, l'entrave au droit d'accès et de communication, l'entrave au droit de rectification, sont punies des peines prévues pour les contraventions de 5ème classe ;

possibilité d'engager la responsabilité de la personne morale : article 226-24 du Code pénal.

Commentaires

Les poursuites pénales pour non respect de la loi Informatique et Libertés demeurent rares.

On peut citer un arrêt ayant condamné le Président d'un syndicat de médecins du travail pour défaut de prise des précautions utiles pour empêcher la communication d'informations médicales à du personnel administratif tiers non autorisé, au motif notamment qu'il n'avait pas fait assurer une formation suffisante pour que chacun connaisse parfaitement le fonctionnement du système (Chambre Criminelle de la Cour de cassation 30 octobre 2001).

Un projet de loi actuellement en cours d'examen par le Parlement français va modifier les dispositions de la loi Informatique et Libertés. Ce projet vise notamment à transposer en droit français les dispositions de la directive européenne n° 95/46/CE relative aux données personnelles (voir fiche de lecture sur la directive 95/46).

Le projet de loi a été adopté par le Sénat en première lecture le 1er avril 2003, après une 1ère lecture par

l'Assemblée Nationale sous la précédente législature. Il doit revenir pour un vote définitif devant l'Assemblée Nationale.
Le nouveau texte modifiant la loi Informatique et Libertés pourrait être adopté en 2004.

Outre l'intégration en droit français des dispositions de la directive, le futur texte augmentera les pouvoirs de contrôle a posteriori de la CNIL sur la mise en œuvre des traitements, qui s'exercent principalement à l'occasion des formalités préalables. Elle se voit accorder un droit d'accès aux locaux et établissements où sont mis en œuvre des traitements de données à caractère personne, entre 6 et 21 heures (article 44).

Le projet précise que seul un médecin peut requérir communication des données médicales.

La CNIL se verra également accorder le pouvoir, après mise en demeure, de prononcer des sanctions pécuniaires, et d'ordonner la cessation d'un traitement. En cas d'urgence, elle pourra décider l'interruption du traitement pour une durée de trois mois, ou informer le Premier Ministre pour qu'il prenne les mesures nécessaires (pour les traitements relatifs à des infractions pénales ou qui concernent la sûreté de l'Etat, la défense ou la sécurité publique).
Elle pourra également saisir les juridictions compétentes.

Dans le projet de loi (article 11), la CNIL se voir également accorder le pouvoir de donner un avis sur la conformité aux dispositions de la loi des projets de règles professionnelles et des produits et procédures tendant à la protection des personnes à l'égard du traitement de données à caractère personnel qui lui sont soumises. Elle pourra également délivrer des labels à des produits ou procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

Fiche de lecture

Désignation du texte	Recommandation de la CNIL sur le traitement des données de santé à caractère personnel		
Réf du texte	Délibération n°97-008	Date du texte	4 février 1997
Auteur(s) / Origine	CNIL		
Zone géo. concernée	France et TOM		
Population, structures et organismes concernés	Professionnels de santé et organismes intéressés par les informations relatives à l'activité médicale et les dépenses de santé.		
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	

Objet, périmètre et limites du texte

Ayant constaté le développement de pratiques consistant à recueillir auprès des professionnels de santé, des données relatives à leurs prescriptions et à leur pratique médicale, la CNIL a souhaité rappeler et préciser dans une recommandation les garanties à respecter lors du traitement et de la transmission de données à caractère personnel relatives à la santé.

Synthèse du texte

La CNIL rappelle que les données de santé à caractère personnel ne peuvent être utilisées que dans l'intérêt direct du patient et que leur exploitation à des fins commerciales est proscrite.

La CNIL rappelle également que, hormis les cas prévus par la loi, les professionnels de santé ne peuvent transmettre à des tiers les données de santé à caractère personnel relatives à leurs patients : **les données transmises ne peuvent l'être que de façon anonymisée.**

Conformément à l'article L 365-2 du CSP, si une exploitation commerciale des données est envisagée, l'obligation d'anonymisation s'étend aux données qui permettent d'identifier le médecin prescripteur.

La CNIL insiste enfin sur trois points qui lui paraissent importants :

- l'information et le respect des droits des personnes
- la confidentialité des informations et la sécurité des traitements.
- l'adéquation entre les données traitées et la finalité poursuivie.

Concernant l'information, la CNIL recommande que les professionnels de santé susceptibles de participer à des systèmes d'informations médicales et de transmettre des données soient clairement informés :

- de l'identité de l'organisme responsable du système ;
- de ses finalités ;
- des conséquences à leur égard de leur participation ;
- des destinataires des informations transmises ;
- des modalités d'exercice de leurs droits d'accès ;
- en cas de mise à disposition du professionnel de santé de moyens informatiques par l'organisme tiers, les contrats conclus doivent bien préciser les modalités de cette mise à disposition et le sort des données en fin de contrat.

La CNIL rappelle également que lorsque les professionnels de santé transmettent des données directement ou indirectement nominatives concernant leurs patients à des tiers habilités, ils doivent en informer leurs patients, afin que ces derniers puissent le cas échéant, exercer leur droit d'opposition (applicable sauf dans les cas où la transmission est imposée par la loi).

Concernant la sécurité, la CNIL rappelle l'importance de :

- préserver la sécurité des informations relatives à l'état de santé ;
- garantir l'anonymisation des données ;
- prévoir des clauses contractuelles appropriées.

En cas de télétransmission, les professionnels de santé doivent pouvoir disposer des moyens techniques nécessaires pour vérifier l'effectivité des mesures prises.

Commentaires

Cette recommandation se limite à rappeler et synthétiser de manière générale les dispositions applicables pour les professionnels de santé en matière de traitement de données de santé.

Fiche de lecture

Désignation du texte	Directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et projet de loi de transposition			
Réf du texte	Directive 95/46	Date du texte	24 octobre 1995	
Auteur(s) / Origine	Parlement Européen et Conseil de l'Union européenne			
Zone géo. concernée	Union européenne			
Population, structures et organismes concernés	Etats membres			
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	24 octobre 1998	

Objet, périmètre et limites du texte

La directive 95/46 réglemente les traitements de données à caractère personnel, avec pour objectifs l'établissement d'un haut niveau de protection des personnes, tout en permettant la libre circulation des données personnelles au sein de l'Union européenne.

Elle pose les principes applicables en matière de collecte et de traitement de données à caractère personnel. Ces principes sont communs à tous les membres de l'Union européenne.

La directive contient des dispositions spécifiques aux données médicales (voir infra, synthèse du texte).

Elle contient également des dispositions relatives aux transferts de données personnelles dans d'autres pays, qui ne sont pas examinées dans le cadre de cette fiche de lecture.

Un projet de loi actuellement en cours d'examen par le Parlement français va modifier les dispositions de la loi Informatique et Libertés, en vue notamment de transposer en droit français les dispositions de la directive européenne n° 95/46/CE relative aux données personnelles.

Le projet de loi a été adopté par le Sénat en première lecture le 1er avril 2003, après une 1ère lecture par l'Assemblée Nationale sous la précédente législature. Il doit revenir pour un vote définitif devant l'Assemblée Nationale.

Le nouveau texte modifiant la loi Informatique et Libertés pourrait être adopté d'ici la fin de l'année 2004.

Les dispositions du projet de loi correspondant aux dispositions de la directive seront présentées parallèlement aux principales dispositions de la directive.

L'article 8 du projet de loi a été modifié par les sénateurs afin d'intégrer l'idée figurant dans le §2 de la directive qui indique que les Etats membres peuvent prévoir que le consentement exprès de la personne concernée ne suffit pas. Ceci afin d'éviter que des banquiers, assureurs ou employés puissent, au seul motif qu'ils auraient obtenu le consentement de l'intéressé, procéder à un traitement de données sensibles et notamment de données de santé.

La nouvelle rédaction du texte prévoit qu'il peut être dérogé à l'interdiction de collecte des données sensibles avec le consentement de la personne sauf dans le cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée :

(Article 8 I 1° A (nouveau) Les traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que l'interdiction visée au I ne peut être levée par le consentement de la personne concernée)

Synthèse du texte

1) Notion de donnée à caractère personnel et de traitement – responsable du traitement

Une donnée à caractère personnel est toute information concernant une personne physique identifiée ou identifiable, directement ou indirectement (article 2 a) de la directive).

Comme dans la loi de 1978, la notion de traitement est très large :
« toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »

Projet de loi :

L'article 2 du projet reprend les définitions de la directive.

L'article 3 du projet précise que le responsable du traitement est la personne, l'organisme ou l'autorité publique qui détermine ses finalités et ses moyens.

Il précise également la notion de destinataire d'un traitement : toute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant.

2) Principes applicables à la qualité des données traitées

Ces principes sont les suivants :

les données doivent être traitées loyalement et licitement ;
principe de finalité : les données sont collectées pour des finalités déterminées, explicites et légitimes ;
principe de pertinence et d'exactitude: les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ; elles doivent être exactes et si nécessaire, mises à jour ;
principe du droit à l'oubli : la durée de conservation doit être en rapport avec la finalité ;
principe d'interdiction du traitement des données dites sensibles sans le consentement explicite de la personne concernée.

Projet de loi :
Ces principes sont repris à l'article 6 du projet et à l'article 8 pour les données sensibles.

3) Principes applicables au traitement

Un traitement de données ne peut être effectué que si une des conditions suivantes est remplie :

consentement indubitable de la personne concernée ;
traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles ;
nécessaire au respect d'une obligation légale ;

le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice d'une mission publique ;
le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par les tiers auxquels les données sont communiquées, sous réserve de ne pas porter atteinte à l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Projet de loi :
Ces principes sont repris à l'article 7 du projet de loi.
La notion d'intérêt vital concerne la sauvegarde de la vie de la personne concernée dans le projet de loi.

4) Cas des données relatives à la santé

Ces données font partie des données sensibles dont le traitement est interdit sans le consentement explicite de la personne concernée.

Les exceptions à ce principe applicables en matière médicale sont les suivantes :

le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée dans le cas où la personne concernée se trouve dans l'incapacité de donner son consentement ;
le traitement des données est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion des services de santé et si le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente.

Projet de loi :

Ces principes sont repris à l'article 8 du projet de loi.

L'exception au consentement exprès de la personne couvre les traitements nécessaires à la sauvegarde de la vie humaine auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle, et les traitements nécessaires aux fins de médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion des services de santé et mis en œuvre par un membre d'une profession de santé ou par une autre personne soumise à l'obligation de secret professionnel.

Le projet de loi ajoute des exceptions par rapport à la liste donnée par la directive : les traitements nécessaires à la recherche dans le domaine de la santé et les traitements justifiés par l'intérêt public.
Les exceptions au principe de l'interdiction ne sont valables que dans la mesure où la finalité du traitement l'exige.

5) Droits de la personne concernée

Elle bénéficie d'un droit à l'information et d'un droit d'accès aux données (articles 10 à 12 de la directive).

Elle bénéficie également, sauf disposition contraire du droit national, d'un droit d'opposition à ce que des données la concernant fassent l'objet d'un traitement (article 14 de la directive).

Projet de loi :

Ces principes sont repris aux articles 32 (information) et 38 (droit d'opposition) et 39 (droit d'accès).

Le droit d'opposition ne s'applique pas lorsqu'il a été écarté par une disposition expresse de l'acte autorisant le traitement.

6) Confidentialité et sécurité des traitements

Les obligations relatives à la confidentialité et à la sécurité des traitements sont détaillées aux articles 16 et 17 de la directive.
Le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.
Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

La directive définit de manière précise les obligations incombant aux prestataires traitant des données pour le compte du responsable du traitement.

L'article 16 relatif à la confidentialité des traitements prévoit que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instructions du responsable du traitement.

L'article 17 relatif à la sécurité des traitements prévoit que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et qu'il doit veiller au respect de ces principes.
L'article 17.3 précise que la réalisation de traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur instruction du responsable du traitement et que les obligations de sécurité définies par la législation du pays membre dans lequel le sous-traitant est établi, incombe également à celui-ci.

Projet de loi :

Les dispositions relatives à la confidentialité et à la sécurité ont été reprises aux articles 34 et 35 du projet de loi.

7) Notifications

L'article 18 de la directive prévoit des obligations de notifications à l'autorité de contrôle (en France, la CNIL) préalablement à la mise en œuvre d'un traitement.

La directive prévoit des possibilités de simplification de la notification ou des dérogations pour les traitements qui compte tenu des données à traiter ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées ou lorsque le responsable du traitement désigne un détaché à la protection des données personnelles.

Projet de loi :

Les traitements devront faire, comme dans le système actuel, l'objet de formalités préalables auprès de la CNIL. Par dérogation, certains traitements sont dispensés de déclarations, d'autres traitements devront faire l'objet d'une autorisation préalable de la CNIL.
La distinction entre secteur public (procédure de demande d'avis dans le système actuel) et privé (déclaration) est en revanche supprimée.

L'article 22 du projet prévoit que les traitements pour lesquels le responsable du traitement a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer le respect des dispositions de la loi sont dispensés de formalité préalable. Ces dispositions visent à introduire en droit français les dispositions de la directive relatives au détaché à la protection des données personnelles.

Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Cette disposition permettra de déterminer un seul responsable du traitement même lorsque différents établissements sont concernés.

L'autorisation préalable de la CNIL concerne notamment les traitements suivants (la présente liste n'est pas exhaustive) :

traitements justifiés par l'intérêt public ;
traitements portant sur des données génétiques (sauf ceux mis en œuvre par des médecins ou biologistes et nécessaires à l'exercice médical – prévention, diagnostic – administration des soins ou traitements) ;
interconnexion de fichiers dont les finalités sont différentes ;
traitements portant sur le n° d'inscription au répertoire national d'identification des personnes physiques. Lorsque ces traitements sont mis en œuvre pour le compte de l'état ou d'un organisme gérant un service public, ils sont autorisés par décret en Conseil d'Etat pris après avis de la CNIL.

Commentaires

La France a accumulé un retard important dans la transposition de la directive du 24 octobre 1995, puisque celle-ci aurait dû intervenir avant octobre 1998.

Un des principaux apports attendu du projet de loi est le renforcement des pouvoirs de la CNIL (voir fiche sur la loi de 1978).

Le système de déclaration des traitements n'est pas simplifié, au contraire, puisque selon les cas les traitements relèvent cinq régimes différents (contre trois actuellement) : déclaration, dispense de déclaration, déclaration simplifiée, autorisation, acte réglementaire pris après avis de la CNIL

Concernant les données relatives à la santé, l'apport principal de la directive et donc du projet de loi est de ranger ces données parmi les données sensibles avec le principe de l'interdiction de traitement sans le consentement exprès, principe assorti toutefois d'exceptions pour le secteur médical

Fiche de lecture

Désignation du texte	Etude concernant l'identification du patient			
Réf du texte	AFNOR S95N N 793	Date du texte	31 mars 2002	
Auteur(s) / Origine	Groupement pour la Modernisation du Système d'information Hospitalier			
Zone géo. concernée	France et territoires d'outre mer			
Population, structures et organismes concernés	Etablissements publics et privés de santé			
Mise en oeuvre du texte	applicable ☒ appliqué ☐	date de mise en application	N/A	

Objet, périmètre et limites du texte

Le système de santé se doit d'améliorer la prise en charge des patients en terme de prévention, de qualité et de continuité des soins. Pour un problème de santé, le patient est souvent pris en charge par plusieurs organisations de santé (établissement de santé, secteur libéral, réseaux de soins…) et donc par de multiples professionnels de santé qui doivent travailler en étroite coopération. Les informations de santé d'un patient sont donc produites et contenues dans des systèmes distribués, sous des identités différentes, ce qui complique l'échange et le partage du dossier patient. De plus, dans les bases de données de ces différents systèmes apparaissent des doublons, des collisions, qui entachent la qualité de l'identification et peuvent être à l'origine d'erreurs potentiellement graves.
Pour résoudre ce problème et être en mesure d'atteindre une qualité optimale dans le processus de gestion de l'identification, différentes solutions complémentaires ont été étudiées : les solutions à base d'identifiant unique et celles à base d'identifiants multiples. Ces dernières sont fondées sur la notion de rapprochement d'identités, basée sur quatre types d'architectures mettant en œuvre les principes de corrélation et de fédération. Dans cette analyse ont été prises en compte trois types de contraintes :

- les contraintes réglementaires pesant notamment sur l'utilisation du *Numéro d'Inscription au Répertoire* (NIR) ou d'un *Identifiant Permanent de Santé* (IPS),
- les contraintes techniques relevant des systèmes actuellement utilisés dans les systèmes d'information de santé (qui produisent leurs propres identifiants)
- les contraintes organisationnelles permettant d'assurer la qualité du processus d'identification.
- Dans ce contexte, ont été définis les principes d'une infrastructure permettant l'identification fiable du patient, des recommandations organisationnelles à l'attention des établissements de santé ainsi que les spécifications fonctionnelles des composants d'infrastructure ou « services » d'identification, valables à l'intérieur de l'établissement de santé mais aussi dans le cadre de la coopération entre organisations de santé.

Les principes techniques et organisationnels d'une infrastructure d'identification et de rapprochement sont décrits ci-après.

Synthèse du texte

Etat de l'art

L'utilisation d'un identifiant unique apparaît, à première vue, comme la seule solution permettant d'identifier de manière fiable un patient. Cette solution paraît d'autant plus simple à mettre en oeuvre qu'il existe déjà en France, comme dans d'autres pays, un numéro d'identification d'une grande partie de la population. Il s'agit du *Numéro d'Inscription au Répertoire* (NIR[3]) *National d'Identification des Personnes Physiques* (RNIPP). Ce numéro est déjà utilisé par l'INSEE, la CNAM, le Ministère des finances, pour y indexer des données de nature administratives ou financières. Il existe cependant des contraintes réglementaires quant à l'utilisation du NIR dans la sphère de santé ; la CNIL a pour mission de veiller au respect des libertés individuelles.

La solution qui pourrait être construite à partir d'un *Identifiant Permanent de Santé* (IPS) créé lors de la première entrée du patient dans le système de santé et utilisé par la suite au cours de ses contacts ultérieurs est une autre solution basée sur un identifiant unique. Cependant, comme pour le NIR, elle requiert une modification importante des processus d'identification et des équipements en place dans les établissements. D'autre part la mise en place d'un IPS nécessite de déterminer quelle structure est en charge de la gestion de l'IPS au niveau national.

Des associations de citoyens, particulièrement sensibles à la protection des droits individuels des personnes se mettent en place comme dans d'autres pays occidentaux. Elles sont en droit de s'opposer à l'utilisation généralisée d'un identifiant unique, rendant une telle pratique difficilement envisageable à court ou moyen terme.

Des approches pragmatiques et alternatives se sont développées. Le standard PIDS (*Person Identification Services*) de l'Object Management Group (OMG) et plus précisément du sous-groupe CORBAmed propose une définition des traits d'identification et introduit un certain nombre de concepts permettant de définir un modèle d'infrastructure d'identification basé sur la corrélation d'identités, c'est à dire la mise en correspondance des identités existantes produites par les applications en place. Il existe une dizaine de produits, principalement aux Etats Unis, qui ont été développés selon ce standard.

La plupart des établissements de santé utilise des identifiants multiples pour assurer le suivi de leurs patients. Ces identifiants sont produits par les applications « métiers » utilisées dans les différents services des établissements : gestion administrative du patient, systèmes de gestion de laboratoire, logiciels de production de soins, etc. Un grand nombre d'établissements dispose d'un index central d'identités patient qui produit un *Identifiant Permanent du Patient* (IPP) pour chaque patient pris en charge. L'IPP est généralement transmis aux différentes applications métiers pour assurer la continuité de l'identification du patient au sein de l'établissement. Cependant, la nécessité d'une interface entre les applications métier et l'index des identités reste encore bien souvent un problème (définition, mise en œuvre, maintenance) et la qualité des index sujette à l'apparition de doublons d'identités. De plus, au sein des établissements, des mesures organisationnelles existent mais sont plus ou moins bien formalisées : procédures d'identification, sensibilisation et formation des utilisateurs au regard de l'identification, gestion de la qualité de l'index et suppression des doublons.

Résultats de l'étude

Définitions

Identité

L'identité patient comprend les éléments suivants :

- L'identifiant du patient représenté par une séquence de caractères. C'est un élément technique qui permet de repérer le patient dans le système d'information ;
- Le profil du patient qui rassemble les informations permettant de le décrire : nom, prénom, date de naissance, sexe par exemple.

Le profil est composé de traits qui représentent les propriétés du patient. On distingue les traits stricts, les traits étendus et les traits complémentaires.

L'accès à ces traits est soumis à autorisation. Les niveaux d'autorisation peuvent être plus ou moins étendus pour permettre l'accès à tout ou partie des traits.

Les traits stricts permettent l'identification du patient. Il est recommandé d'utiliser au minimum les traits suivants : Nom de famille, Nom d'usage, Nom marital, Prénoms, Date de Naissance et Sexe.

Les traits étendus permettent la vérification de l'identité du patient. A titre d'exemple, on peut citer les traits de type administratif (alias, adresse, numéro de téléphone,…) ou de type médical (groupe sanguin, allergie connue, …).

Les traits complémentaires sont des informations plus confidentielles fournies par les applications connectées au système d'identification (dossier médical, dossier de soins, etc.). Leur accès est limité aux professionnels habilités. Ils ne sont utiles que lorsqu'il subsiste un doute sur l'identification d'un patient après consultation des traits stricts et étendus. Il s'agit de données « métier ». On pourra aussi y trouver les données de type biométrique (fond de l'œil, empreinte digitale, …).

Domaine d'identification

Un domaine d'identification D représente un ensemble d'identifiants opérationnels avec une unicité souhaitée de l'identifiant patient. On peut citer par exemple l'ensemble des IPP gérés par le SIH d'une organisation hospitalière. Le nom d'un domaine est unique.

Un identifiant ID est valide dans un domaine D. Il est défini par le processus ayant pour objet d'identifier une personne à laquelle on attribue un identifiant et se déroulant dans une organisation.

Un domaine d'identification dispose au moins des services suivants :

- recherche sur identifiant ;
- recherche sur traits ;
- gestion de l'identité (création d'identifiants, résolution de doublons, de collisions, modification des traits, …).

Une identité y est représentée par une strcuture de type D : {ID,[T]} où D est le nom du domaine, ID est l'identifiant dans le domaine, [T] sont les traits du patient.

Domaine de rapprochement

Un domaine de rapprochement rapprochant les domaines d'identification D_1 et D_2 est constitué de l'ensemble de couples d'identifiants ID_1, ID_2 avec unicité souhaitée du couple par personne.

De manière générale, un domaine de rapprochement D_x rapprochant les domaines d'identification D_1, …, D_i, ,…D_n est constitué de l'ensemble de la collection des couples D_i : ID_i ,[T_i] ; D_j : ID_j ,[T_j], avec unicité souhaitée par personne.

Modèles de rapprochement

La mise en relation des identités patient de domaines d'identification différents peut se réaliser selon deux types de modèles, la corrélation et la fédération.

Dans le modèle de corrélation, l'identité enregistrée pour un patient dans un domaine d'identification est rapprochée des identités des autres domaines pour former un ou plusieurs couples d'identifiants faisant partie de la collection d'identités relative aux rapprochements pour ce patient.

Dans le modèle de fédération, l'identité enregistrée d'un patient pour chaque domaine d'identification est rapprochée pour former une collection d'identités relatives à ce patient. Cette collection d'identités est fédérée par une identité unique au sein du domaine de rapprochement. Ces deux modèles peuvent faire l'objet chacun de deux modes de mise en oeuvre : rapprochement de gré à gré ou rapprochement hiérarchique.

Les paragraphes suivants illustrent les différents modèles de rapprochement.

Corrélation Gré à Gré

Dans le cas de la *corrélation gré à gré* (figure 1), le rapprochement d'identités est réalisé dans chacune des structures participant au domaine de rapprochement. Le rapprochement d'identités s'effectue deux à deux sur la base des identités de chaque domaine d'identification. Un état de rapprochement permet de le qualifier.

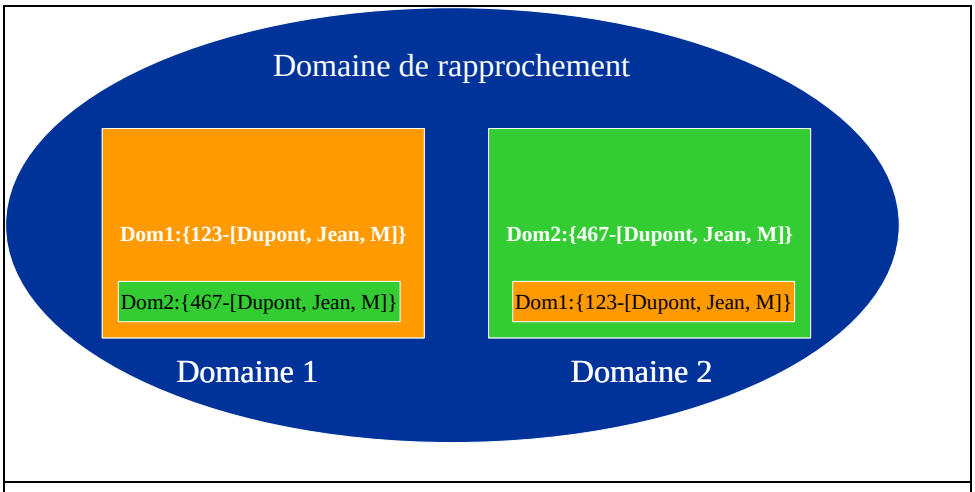


Figure 1 : Rapprochement par corrélation gré à gré

Corrélation Hiérarchique

Dans le cas de la *corrélation hiérarchique* (figure 2), le rapprochement est réalisé dans une structure hiérarchique située au-dessus des domaines d'identification. Le rapprochement d'identités s'effectue deux à deux sur la base des identités de chaque domaine d'identification. Un état de rapprochement permet de le qualifier.

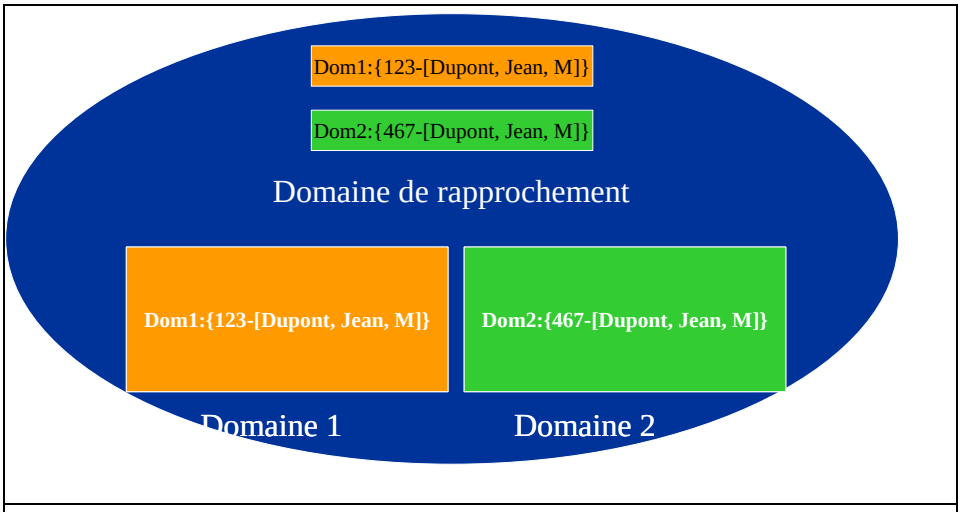


Figure 2 : Rapprochement par corrélation hiérarchique

Fédération Gré à Gré

Dans le cas de la *fédération gré à gré* (figure 3), le rapprochement d'identités est réalisé dans chacune des structures participantes au domaine de rapprochement. Le rapprochement d'identités s'effectue deux à deux sur la base d'une identité fédératrice et d'une identité d'un domaine d'identification. Un état de rapprochement permet de le qualifier.

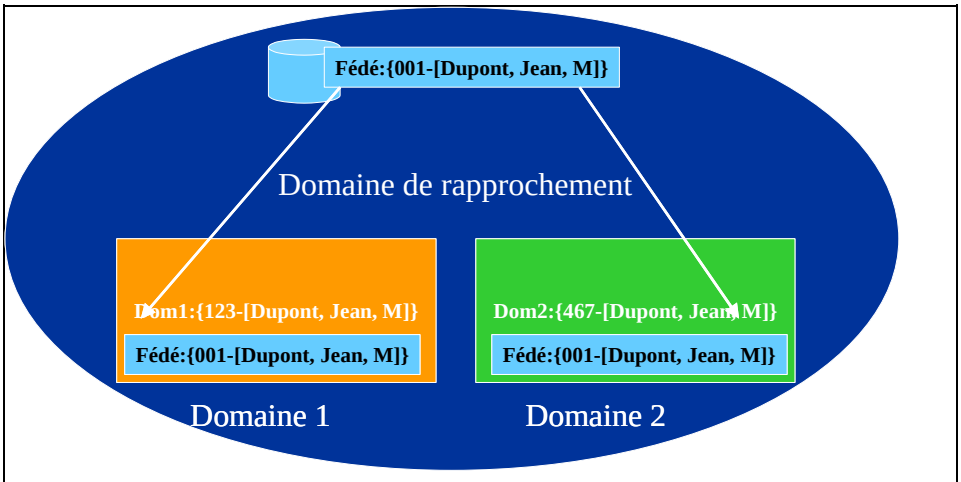


Figure 3 : Rapprochement par fédération gré à gré

Fédération Hiérarchique

Dans le cas de la *fédération hiérarchique* (figure 4), le rapprochement d'identités s'effectue dans une structure hiérarchique située au-dessus des domaines de rapprochement. Les rapprochements d'identités s'effectuent deux à deux sur la base d'une identité fédératrice et d'une identité d'un domaine d'identification. Un état de rapprochement permet de le qualifier.

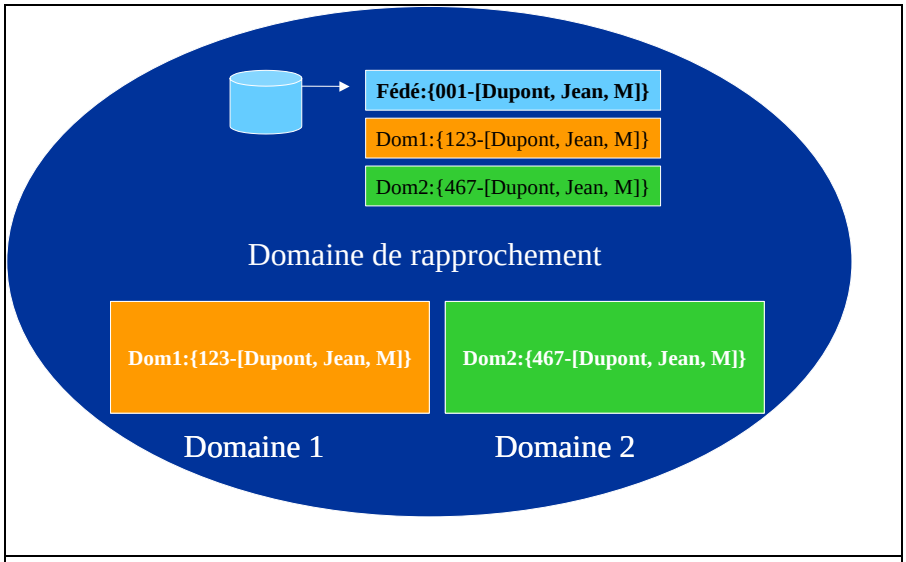


Figure 4 : Rapprochement par fédération hiérarchique

Politiques d'identification et de rapprochement

Lorsque des organisations de santé souhaitent mettre en place un domaine d'identification ou un domaine de rapprochement, elles doivent déterminer les orientations qui leur semblent les mieux adaptées en fonction de l'environnement, des pratiques en terme d'identification, de leurs moyens et de la finalité des échanges concernés.
Chaque organisation de santé doit donc définir une politique d'identification. Lorsque plusieurs organisations de santé se regroupent pour former un domaine de rapprochement, elles définissent une politique de rapprochement.

La politique d'identification

Chaque établissement définit une politique d'identification qui lui est propre. L'élaboration de la charte est placée sous la responsabilité d'une instance nommée *Autorité de Gestion de l'Identification* (AGI). L'AGI est constituée des représentants de la direction de l'établissement, de la Direction des systèmes d'information, du Médecin du DIM et de représentants des différents services de l'établissement.

Cette politique d'identification s'applique à l'ensemble des domaines d'identification faisant éventuellement partie de l'organisation de santé.

La charte d'identification contient l'ensemble des éléments organisationnels et techniques nécessaires pour appréhender l'identification au sein d'une organisation de santé. Elle constitue un préalable indispensable à la participation à un domaine de rapprochement.

La charte d'identification détaille les éléments suivants :

- La description du périmètre de l'établissement (les structures, les applications informatiques et les personnels concernés) ;
- Les instances en charge de l'identification (leur mission, leur mode de fonctionnement) ;
- Le mode d'échange d'informations entre les différentes applications informatiques concernées ;
- L'identification (format, composition…) ;
- Les processus internes d'identification (règles de gestion) ;
- La sécurité ;

- Les critères d'analyse de la qualité du système ;
- Les moyens techniques utilisés.

La politique d'identification définie par l'AGI est mise en œuvre par l'ensemble des personnels concernés au sein de l'établissement.

Une cellule d'identito vigilance (CIV) est créée pour aider à la mise en œuvre opérationnelle de la politique d'identification. Cette CIV constitue le support opérationnel des services concernés par l'identification. En cas de problème d'identification, elle détermine les actions correctrices à conduire. Elle rapporte à l'AGI les éléments permettant de vérifier la bonne application de la politique d'identification.

La politique de rapprochement

Chaque domaine de rapprochement élabore une politique de rapprochement qui lui est propre. L'adhésion à un domaine de rapprochement est volontaire.

Cette politique s'applique à l'ensemble des organisations de santé qui adhérent au domaine de rapprochement. Elle définit les responsabilités et les règles d'échanges d'informations entre chacune de ces organisations.

La rédaction de la charte de rapprochement est placée sous la responsabilité d'une instance nommée *Autorité de Gestion des Rapprochements* (AGR). Cette instance a en charge l'élaboration de la politique de rapprochement.

La charte de rapprochement reprend les mêmes éléments que la charte d'identification mais pour le niveau du domaine de rapprochement. Elle détaille les éléments suivants :

- La description du périmètre du domaine de rapprochement (les établissements concernés) ;
- Les instances en charge du rapprochement (leur mission, leur mode de fonctionnement) ;
- Le mode d'échange d'informations au sein du domaine de rapprochement ;
- L'identification (format, composition…) ;
- Les processus de rapprochement (règles de gestion) ;
- La sécurité ;
- Les critères d'analyse de la qualité du système ;
- Les moyens techniques utilisés.

La politique définie par l'AGR est mise en œuvre par l'ensemble des personnels des établissements concernés par le rapprochement.

Une cellule d'identito vigilance du domaine de rapprochement (CIVR) est créée pour aider à la mise en œuvre de la politique de rapprochement. Elle assiste les domaines d'identification pour la mise en œuvre de l'ensemble des services de rapprochement et le suivi des rapprochements.

Commentaires

Dans le cadre de la modélisation du processus d'identification, a été spécifié le composant d'infrastructure concernant l'identification du patient permettant de contribuer à la continuité des soins et à la traçabilité des patients au sein des SIH et plus généralement dans le cadre des SI des différentes organisations de santé (regroupement d'établissements, réseaux de santé etc.). Ces recommandations sont compatibles avec l'emploi d'identifiants existants au sein des organisations et permettent également d'utiliser, complémentairement, des identifiants de portée plus large, tels que les identifiants nationaux ou européens. L'utilisation d'un identifiant national unique, peut être envisagée selon deux options.

La première est l'*option identification*. Dans cette option, les organisations de santé constituent des domaines rapprochés par un domaine national par fédération gré à gré. Ce domaine national dispose d'un index national qui est le référentiel contenant les identités patient. Dans ce cas, les identifiants produits par les applications des SIH doivent être remplacés par l'identifiant national provenant de l'index national. Cette solution semble lourde à mettre en œuvre car elle implique, d'une part, une adaptation forte des applications actuellement utilisées dans les SIH (modification du format de l'identifiant et des traitements associés) et, d'autre part, une reprise des index existants pour remplacer les identifiants locaux par l'identifiant national.

La seconde est l'*option de rapprochement.* Dans ce cas les organisations de santé constituent des domaines rapprochés par un domaine national par fédération gré à gré. Ce domaine « national » dispose d'un index « national » qui est le référentiel contenant les identités patient. Dans cette option, l'identifiant national est alors considéré comme un « trait supplémentaire » permettant de fiabiliser l'identité du patient. L'identifiant opérationnel reste celui produit par les applications du système d'information hospitalier. L'avantage de cette solution est qu'elle génère peu d'adaptation des applications actuellement utilisées dans les SIH.

Les avantages des solutions à base de rapprochement sont, principalement, la prise en compte de l'ensemble des identités existantes et la possibilité de mise en œuvre progressive.

Les modèles de rapprochement étudiés ont déjà fait l'objet d'une mise en œuvre opérationnelle dans certaines institutions de santé. La fédération gré à gré est appliquée dans le cadre des systèmes d'information hospitaliers (communication de l'IPP produit par le serveur d'identité vers les applications métiers : systèmes de gestion de laboratoire, logiciels des unités de soins…). Les modèles hiérarchiques sont à la base des EMPI (*Enterprise Master Patient Index*) implantés aux Etats Unis mais aussi en Europe (Hôpitaux cantonaux de Lausanne).

Les modèles nécessitant qu'une structure technique soit mise en œuvre pour le domaine de rapprochement sont plus lourds que celui basé sur la corrélation gré à gré qui requiert une adaptation des systèmes utilisés dans les domaines d'identification. Cependant ces modèles correspondent mieux à des domaines de rapprochement impliquant un grand nombre d'organisations de santé.

Le choix du modèle dépend fortement d'un certain nombre de paramètres liés à la nature du projet de communication d'informations entre professionnels qui sous-tend le besoin de partage des identités. Les objectifs du projet, la nature des organisations de santé à rapprocher, leur nombre, les moyens humains et techniques pouvant être mis à disposition permettent d'orienter le choix vers un modèle plutôt qu'un autre.

A.1.3 Certification et contrôle

Fiche de lecture

Désignation du texte	Evaluation et certification de la sécurité offerte par des produits et systèmes des TI		
Réf du texte	Décret 2002-535	Date du texte	18 avril 2002
Auteur(s) / Origine	Le gouvernement français		
Zone géo. concernée	France, Nelle Calédonie, Polynésie, Wallis, Futuna, Mayotte		
Population, structures et organismes concernés	DCSSI, Commanditaire, Centre d'évaluation		
Mise en oeuvre du texte	applicable ☒ appliqué ☐	date de mise en application	2002

Objet, périmètre et limites du texte

Ce texte explicite les critères et conditions à réaliser en vue de l'évaluation et la certification de la sécurité offerte par des produits et systèmes des technologies de l'information.

Il précise en particulier :

1. Les procédures retenues en vue de :

. l'évaluation,
. la certification.

2. Les critères d'agrément des Centres de certification

3. Le périmètre de responsabilité du Comité Directeur de la Certification des Technologies de l'Information
(DCSSI)

4. Un ensemble de dispositions diverses et transitoires.

Synthèse du texte

La sécurité offerte par des produits et systèmes des technologies de l'information peut être certifiée dans les conditions suivantes :

Un commanditaire en fait la demande à la DCSSI et transmet un dossier d'évaluation en vue de certification.

La DCSSI doit s'assurer que les objectifs de sécurité sont définis de manière pertinente au regard des normes, prescriptions techniques et règles de bonnes pratiques.

Le commanditaire peut choisir le centre d'évaluation et doit fournir tous les éléments nécessaires au bon accomplissement des travaux.

Le commanditaire et la DCSSI valident les rapports d'évaluation en liaison avec le centre d'évaluation

Ce rapport peut donner lieu à la délivrance d'un certificat ou à un refus de certification.

Commentaires

Le schéma de certification auquel il est fait référence ici, est désigné par le Schéma Français d'Evaluation et de Certification de la Sécurité des Technologies de l'Information. Il est précisément décrit dans les documents
ECF00, ECF01, ECF02, ECF03, ECF04, ECF11 et ECF12 disponibles en ligne auprès de la DCSSI (www.ssi.gouv.fr). Les normes sur lesquelles il s'appuie offrent un cadre complet et rigoureux à l'évaluation de produits de sécurité.
Toute l'ambiguïté de ce schéma et les difficultés à l'appliquer résident d'une part dans la notion de Technologies de l'Information (qu'est-ce que cela couvre exactement ?) et dans l'emploi de ce schéma d'évaluation au sein d'autres processus que l'on désigne par labellisation ou qualification.

En ce qui concerne les aspects liés aux Technologie de l'Information, cela couvre, au sens du schéma, un produit ou un système. Un produit est défini de la manière suivante : "paquetage logiciel et/ou matériel TI qui assure une fonctionnalité conçue pour être utilisée ou incorporée au sein de multiples systèmes". Un système prend la définition ci-après : "installation spécifique de TI, avec un but et un environnement d'exploitation particuliers" où TI signifie Technologies de l'Information. Le produit assure une fonctionnalité bien précise, il est incorporé au sein de multiples systèmes, il peut donc être certifié en faisant les hypothèses adéquates sur l'utilisation et l'environnement du produit au sein de ces "multiples systèmes", notamment en ce qui concerne le processus de management de la sécurité permettant une utilisation et un environnement sûrs.

Ces hypothèses sont clairement énoncées au sein de profils de protection ou de cibles de sécurité, dans des sections prévues à cet effet :
"hypothèses sur l'environnement TI" ou "non TI" et "politiques de sécurité applicables". Cf. ISO 15408.

Comment cela s'applique-t-il dans le cas d'un système ? La sécurité d'un système est à la fois caractérisée par les produits qu'il intègre mais aussi par le processus de gestion de la sécurité lié à l'environnement d'exploitation aux modes d'utilisation du système. Il ne peut donc pas être certifié sur la base d'hypothèses sur son utilisation et son environnement d'exploitation. Ainsi, la question est de savoir comment certifier les modes d'utilisation et l'environnement d'exploitation du système. Sur ce point le schéma est incomplet, notamment en raison d'une lacune importante dans les normes.

Néanmoins les expérimentations sont en cours : adaptation des critères communs, normes complémentaires émergeantes (ISO 17799), etc.

L'émergence de la signature électronique a conduit la communauté européenne et la France à bâtir un schéma de qualification des signatures électroniques.
Une partie de ce schéma s'appuie sur la certification des produits employés et la qualification du processus de gestion de la sécurité du système de signature électronique. Par ailleurs, au travers de la DCSSI, l'administration française a souhaité voir labellisés un certain nombre de produits de sécurité qui répondraient à ses propres exigences de sécurité.
Ce processus de labellisation s'appuie aussi sur la certification des produits, sur la base de cibles de sécurité adaptées aux exigences de l'administration.

Fiche de lecture

Désignation du texte	ECF – Schéma Français d'Evaluation et de Certification de la sécurité des technologies de l'information		
Réf du texte	ECF - ITSEC – CC	Date du texte	Mai 1999
Auteur(s) / Origine	ISO – CCEB (Common Criteria Evaluation Borad)		
Zone géo. concernée	Europe – Asie – Australie – Etats-Unis		
Population, structures et organismes concernés	Tous		
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	1995

Objet, périmètre et limites du texte

Des travaux ont été menés depuis les années 80 afin de définir les critères d'évaluation de la sécurité des technologies de l'information.
Ces critères ont pour but de définir les méthodes et les moyens permettant d'exprimer les besoins de sécurité, de les transformer en fonctions de sécurité et de les implémenter pour ensuite procéder à leur évaluation globale.

Historique

La France, l'Allemagne, le Royaume-Uni et la Hollande ont été à l'initiative de la Recommandation Européenne ITSEC (Information Technology Security Evaluation Criteria).

Les ITSEC sont issus des différents travaux de ces pays, respectivement :
Livre Bleu-Blanc-Rouge.
ZSIEC.
Livre Vert.

Essentiellement tournés vers l'évaluation des produits, les ITSEC ne procèdent pas à la séparation des fonctions et de l'assurance ainsi qu'à la nécessité de disposer d'un standard d'évaluation de la sécurité des systèmes d'information tel que le demande le marché global.

D'autres travaux, dans un contexte international, ont été menés ; on peut citer :

TCSEC – Etats Unis.
CTCPEC – Canada.
FCITS – Etats Unis.
JCSEC – Japon.

Objet, périmètre et limites du texte

La recherche d'une reconnaissance internationale de ces différents travaux a donné naissance aux Critères Communs (Common Criteria). Contrairement aux ITSEC, les critères communs mettent en œuvre des notions fondamentales permettant de répondre à la demande du marché :

Environnement de sécurité.
Objectifs de sécurité.
Détermination des exigences fonctionnelles.
Détermination des exigences d'assurance.
Evaluation.

Ces Critères Communs vont permettre de satisfaire les différents niveaux de responsabilité dans l'entreprise en matière de définition de la politique de sécurité.

Sept organisations internationales sont à l'origine des ces critères communs :

BSI – Allemagne.
CESG – Royaume Uni.
CSE – Canada.
NSA – Etats Unis.
NIST – Etats Unis.
SCSSI – France.
NLNCSA – Pays Bas.

Chacune de ces organisations est garante de la mise en œuvre des procédures permettant l'évaluation et la certification de la sécurité des technologies de l'information.

En parallèle l'ISO débuta en 1990 ses travaux sur des critères d'évaluation internationaux à usage général sous la dénomination ISO/IEC JTC 1/SC 27/WG3.

La version V2 des Critères Communs a été officialisée en mai 1998 et présentée par la DCSSI en septembre 1998 aux industriels français. Cette même année une reconnaissance mutuelle sur l'évaluation de la sécurité a été signée par les sept organisations internationales. Depuis plusieurs pays s'étaient portés candidats à cette reconnaissance ; Pays Bas, Australie, Nouvelle Zélande, Japon, Corée du Sud, Espagne, Finlande, Grèce, Italie, Norvège, Suède, Suisse…

Poussé par les Critères Communs l'ISO à procédé à leur officialisation le 8 juin 1999 sous l'intitulé :

ISO 15408 : Evaluation Criteria for Information Technology Security Evaluation.

Commentaires

ISO 15408 : Les profils de protection :

L'intérêt de la norme est de permettre d'établir des profils de protection. Les éléments issus de l'étude des risques, du choix des objectifs de sécurité et des exigences permet de créer un « catalogue » des mesures de sécurité sur un projet donné. On peut ainsi définir des profils de protection pour des problématiques précises :

Protection des transactions confidentielles.
Sécurité des postes de travail.
Sécurisation Intranet/Extranet.
Etc.

Un projet de sécurisation peut désormais s'encadrer d'un cadre normatif sous la forme de définition d'un profil de protection qui aboutira à la rédaction d'un ensemble de recommandations techniques et non techniques d'où l'on pourra extraire par exemple des manuels sécurité à l'usage des utilisateurs.

ISO 15408 : L'intérêt pour les entreprises

Un des besoins des entreprises est de pouvoir labelliser la sécurité mise en œuvre dans un projet donné. Si cette dernière a été conçue dans l'esprit d'un profil de protection, il est possible d'en effectuer une validation ayant une reconnaissance internationale. C'est un besoin que l'on rencontre particulièrement dans une organisation ou le RSSI doit élaborer des procédures de sécurité qui seront approuvées par les responsables des différentes entités. Le profil de protection est donc l'outil idéal et indispensable pour le responsable sécurité « Corporate ».

Les profils de protection sont aussi des outils pour les responsables qualité et sécurité, leur permettant de disposer de procédures qualité et de procédures sécurité. Le profil de protection met à disposition un document recensant les objectifs de sécurité et leurs exigences indépendamment de l'évolution des technologies.

Ce profil est aussi un outil de décision appréhendant l'évolution des mesures de sécurité et la prise en compte des nouveaux objectifs de sécurité liés à l'évolution du système d'information et des besoins de l'utilisateur.

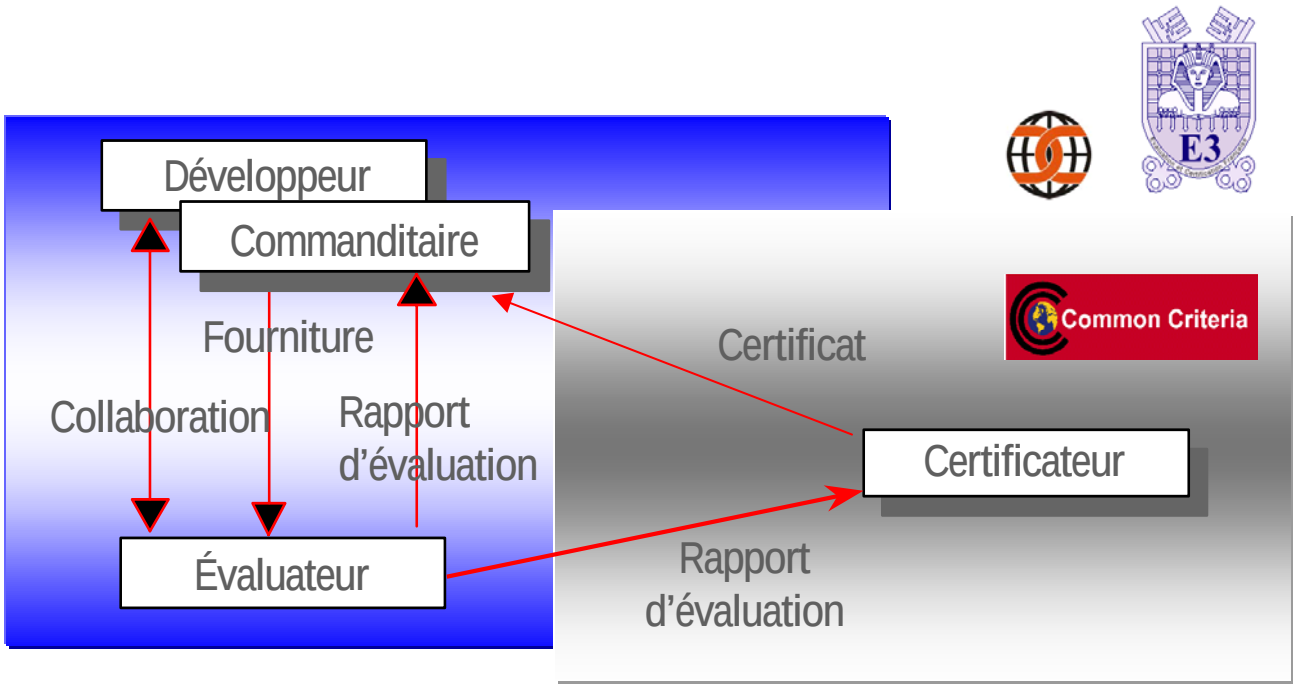
Le schéma d'évaluation et de certification

Un avis du Premier ministre en septembre 1995 officialise le Schéma Français d'Evaluation et de Certification. Ce Schéma met en œuvre les éléments indispensables à la validation du profil de protection. Cette validation aura une valeur internationale. La validation passe par deux étapes :

- Une évaluation du profil de protection par un laboratoire d'essais agréé.
- Une certification donnée par un organisme certificateur.

Le commanditaire ayant rédigé son profil de protection le transmet à un laboratoire d'essais (CESTI – Centre d'Evaluation de la Sécurité des Technologies de l'Information).

Le CESTI effectuera une étude approfondie de ce profil afin d'en contrôler le contenu en particulier en cherchant à valider si les exigences fonctionnelles et d'assurance utilisées sont cohérentes avec les objectifs de sécurité définis. Le cas échéant, le CESTI transmettra un rapport d'évaluation auprès de la DCSSI qui en effectuera la certification; label recherché par les entreprises.



La DCSSI et les CESTI sont les composantes du Schéma Français d'Evaluation et de Certification. Une organisation identique existe dans les principaux pays industrialisés .

A.1.4 Protection contre la fraude

Désignation du texte	Sécurité des systèmes d'information		
Réf du texte	Articles 323-1 à 323-7 du Code pénal	Date du texte	5 janvier 1988 (modifié)
Auteur(s) / Origine	Parlement		
Zone géo. concernée	France et TOM		
Population, structures et organismes concernés	tous		
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	Janvier 1988

Objet, périmètre et limites du texte

Les articles 323-1 à 323-7du Code pénal instituent un ensemble d'incriminations en matière de fraude informatique.

Synthèse du texte

1) Généralités

La fraude informatique concerne, en premier lieu, les accès non autorisés dans les ordinateurs des autres, que ce soit par malveillance, par défi ou par jeu.
La fraude informatique vise, en second lieu, les altérations, dégradations, manipulations de données en tous genres : modifications des données, introduction de virus, sabotages, destructions de documents.
La fraude informatique peut être le fait de personnes extérieures, de tiers, mais le plus souvent de personnes internes à une organisation, un groupement, comme les salariés.

2) Incriminations prévues

2.1) La protection de la confidentialité

Les intrusions
L'intrusion dans un système informatique est traitée par l'article 323-1 alinéa 1 du Code pénal qui précise que :
"Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende".
L'intrusion, c'est le simple fait d'accéder de manière non autorisée, de pénétrer dans le système, mais également le maintien dans le système suite à cet accès. Une personne qui se serait immiscée par erreur dans un système mais s'y serait maintenue de manière consciente rentre ainsi dans le cadre de l'incrimination.

Traditionnellement, on considère que l'exigence de protection du système ne fait pas partie des conditions de l'incrimination.

Les interceptions

L'article 226-15 du Code pénal réprime l'atteinte au secret des communications ainsi que l'installation d'appareils conçus pour réaliser de telles interceptions.
Les atteintes au secret des correspondances réalisées par une personne dépositaire de l'autorité publique dans l'exercice de ses fonctions, de même que de telles atteintes commises par les exploitants de réseaux de télécommunications, les fournisseurs de services de télécommunications sont réprimés par l'article 432-9 du Code pénal.

(voir fiche sur le secret professionnel)

2.2) la protection des données
L'intrusion ayant occasionné des altérations
Lorsqu'une intrusion ou un maintien illicite dans un système a occasionné la suppression, la modification des données contenues dans le système ou une altération du fonctionnement du contenu de ce système, les peines prévues en cas d'intrusion sont aggravées : elles sont portées à deux ans d'emprisonnement et 30 000 euros d'amende (article 323-1 alinéa 2 du Code pénal).
L'atteinte au système
L'article 323-2 du Code pénal dispose que :
"Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 euros d'amende". Les termes généraux utilisés par la loi permettent de sanctionner les altérations diverses telles que la mise en place de bombes logiques, l'introduction de virus, l'envoi massif de courriers électroniques en vue de saturer les serveurs d'un fournisseur d'accès.
L'atteinte aux données
L'article 323-3 du Code pénal prévoit que :
"Le fait d'introduire frauduleusement des données dans un système de traitement automatisé de données ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 euros d'amende".
Le texte sanctionne les altérations volontaires de données, ainsi que les manipulations d'informations, les données fausses introduites sciemment dans un fichier, la modification ou la suppression malveillantes de données sans qu'il ne soit porté atteinte au système informatique lui-même.

Commentaires

Un projet de loi relatif à la confiance dans l'économie numérique, en cours de discussion devant le Parlement, prévoit une augmentation des peines encourues en matière de fraude informatique et la création d'une nouvelle incrimination dite de **fourniture de moyens**, c'est-à-dire que l'on donnerait un cadre juridique pour les poursuites contre ceux qui fournissent les outils servant à commettre les attaques informatiques.
Le projet prévoit (futur article 323-3-1 du Code pénal) :

« Le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçue ou spécialement adaptés pour commettre les faits prévus par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Les dispositions du présent article ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition de l'instrument, du programme informatique ou de toute donnée sont justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de

communications électroniques et des systèmes d'information et lorsqu'elles sont mises en oeuvre par des organismes publics ou privés ayant procédé à une déclaration préalable auprès du Premier ministre selon les modalités prévues par les dispositions du III de l'article 18 de la loi pour la confiance dans l'économie numérique. »

Le bénéfice de l'exception prévue en matière de protection de la sécurité des systèmes d'information nécessitera une déclaration préalable auprès de l'administration.

A.1.5 Confidentialité et secret professionnel

Fiche de lecture

Désignation du texte	Secret professionnel et secret des correspondances par voie de télécoms		
Réf du texte	Articles 226-13,226-14, 226-15 et 432-9 du Code Pénal	Date du texte	10 juillet 1991
Auteur(s) / Origine	Code Pénal		
Zone géo. concernée	France		
Population, structures et organismes concernés			
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	1991

Objet, périmètre et limites du texte

L'article 226-13 du Code pénal est le texte de base relatif au secret professionnel. Le secret médical fait partie des informations couvertes par le secret professionnel.

L'article 226-14 traite des exceptions au secret professionnel.

L'article 226-15 détaille et explicite le délit d'atteinte au secret des correspondances. L'article 432-9 traite des atteintes au secret des correspondances commises par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public et par les fournisseurs de services de télécommunication.

Synthèse du texte

Secret professionnel (article 226-13)

La révélation d'une information à caractère secret par une personne qui en est dépositaire par état ou par profession est punie d'un an d'emprisonnement et de 15 000 € d'amende.
Le principe posé par l'article 226-13 est général et absolu.

Exceptions (article 226-14) :

L'article 226 – 13 n'est pas applicable lorsque la loi impose ou autorise la révélation du secret.
En outre, il n'est pas applicable :
à celui qui informe les autorités administratives, médicales ou judiciaires, de privations ou de sévices, y compris lorsqu'il s'agit d'atteintes sexuelles dont il a eu connaissance et qui ont été infligées à un mineur âgé de moins de 15 ans ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son état physique ou psychique.
au médecin qui avec l'accord de la victime, informe le Procureur de la République de sévices qu'il a constaté dans l'exercice de sa profession et qui lui permettent de présumer que des violences sexuelles ont été commises.

Secret des correspondances

L’article 226 – 15 détaille l’atteinte au secret des correspondances commises de mauvaise foi et en précise les peines (un an d’emprisonnement et 45 000 € d’amende).
Lorsque l’atteinte au secret des correspondances est commise par une personne dépositaire de l’autorité publique ou chargée d’une mission de service public, agissant dans l’exercice ou à l’occasion de ses fonctions ou de sa mission, ou par des exploitants de réseaux de télécommunications, des fournisseurs de services de télécommunications, les peines encourues sont de 3 ans d’emprisonnement et de 45 000 euros d’amende (article 432-9).

A.1.6 Textes généraux

Fiche de lecture

Désignation du texte	Code de la santé publique		
Réf du texte	N/A	Date du texte	N/A
Auteur(s) / Origine	Gouvernement		
Zone géo. concernée	France et territoires d'outre mer		
Population, structures et organismes concernés	Etablissements publics et privés de santé, centres de santé, professionnels de santé		
Mise en oeuvre du texte	applicable ☒ appliqué ☒	date de mise en application	N/A

Objet, périmètre et limites du texte

L'objet et le périmètre du texte sont suffisamment larges pour couvrir à la fois :

- ✓ La protection de la vie privée
- ✓ L'hébergement de données
- ✓ Les responsabilités en matière de sécurité

Les concepts liés à la preuve n'apparaissent pas directement dans les textes.

Cette fiche ne reprend pas l'intégralité des articles de la loi du 4 mars 2002. C'est le cas en particulier des articles liés au concept d'hébergement de données. Se référer aux fiches de lecture (à venir) des décrets d'application qui devraient sortir prochainement.

La limite du texte réside, évidemment, dans le fait que les informations présentées sont des exigences d'ordre légal ou réglementaire. Elles ne fournissent pas de solutions ou de recommandations quant à la mise en œuvre de ces exigences..

La présente fiche est structurée de la manière suivante :

- ✓ La « synthèse » contient 2 parties :

  - L'introduction fournit la liste des articles qui ont fait l'objet d'une lecture
  - La synthèse proprement dite, présente (sans analyse) le contenu des articles lus en donnant entre parenthèses les références à ces articles

- ✓ La partie « commentaires » s'appuie sur le contenu des articles présentés en synthèse, afin de proposer une lecture du code de la santé publique sur les concepts suivants :

  - Organisation des responsabilités vis-à-vis de la sécurité des systèmes d'information de santé
  - Respect de la vie privée dans le domaine de la santé publique
  - Intégrité, disponibilité, authenticité et auditabilité des informations dans le domaine de la santé publique

Synthèse du texte

Cette fiche traite les chapitres suivants :

- ✓ Dans la nouvelle partie législative :
- (Livre 1 sur la protection des personnes en matière de santé / Titre 1, Droits des personnes malades et des usagers du système de santé) Chapitre préliminaire, Droit de la personne, Chapitre 2, Personnes accueillies dans les établissements de santé
- (Livre 5 sur les territoires d'outre mer / Titres 1, Mayotte) Chapitre 1, Droits des personnes malades et des usagers du système de santé
- (Livre 1 sur les professions médicales / Titre 1, Exercice des professions médicales) Chapitre 3, Règles communes d'exercice de la profession
- (Livre 1 sur les établissements de santé / Titre 4, Etablissements publics de santé) Chapitre 2, Organisation hospitalière et universitaire, Chapitre 3, Conseil d'administration et Directeur, Chapitre 7, Dispositions particulières à certains établissements et organismes

- ✓ Dans la partie réglementaire portant sur les décrets en Conseil d'Etat :
- (Livre 7 sur les établissements de santé, le thermoclimatisme et les laboratoires / Titre 1, Etablissements de santé) Chapitre 1A – Section 1 – Sous-section 2, Information des personnes accueillies dans les établissements de santé publics et privés et communication des informations de santé définies à l'article L1111-7, Chapitre 1A – Section 2bis – Sous-section 1 Commission des systèmes d'information sur les établissements de santé, Chapitre 1A – Section 2bis – Sous-section 2 Conditions générales de transmission et d'échange des informations, Chapitre 1A – Section 2bis – Sous-section 3, Accès des tiers au système commun d'information de l'état, des agences régionales de l'hospitalisation et des organismes d'assurance maladie, Chapitre 1A – Section 3, Evaluation et accréditation des établissements de santé

- ✓ Dans la partie réglementaire portant sur les décrets simples :
- (Livre 5bis sur les dispositions relatives aux dispositifs médicaux / Chapitre 1, Dispositions générales) Section 1, Champ d'application et définitions, Section 10, Mise en œuvre de l'obligation de maintenance et de contrôle de qualité
- (Livre 7 sur les établissements de santé, le thermoclimatisme, les laboratoires et les centres de santé / Titre 1, Etablissements de santé) Chapitre 2 – Section 3 Conditions techniques de fonctionnement des établissements de santé, des installations et des activités de soins
- (Livre 7 sur les établissements de santé, le thermoclimatisme, les laboratoires et les centres de santé) Titre 4, Centres de santé
- (Livre 7 sur les établissements de santé, le thermoclimatisme, les laboratoires et les centres de santé / Titre 5, Réseaux et autres services de santé), Chapitre 1er, Réseaux de santé

Organisation relative au système d'information

Cette organisation prend en compte :

- ✓ la commission des systèmes d'information sur les établissements de santé
- ✓ les rôles du conseil d'administration et du Directeur des établissements de santé
- ✓ les modalités de coopération entre établissements
- ✓ la notion de réseaux de santé
- ✓ les universités
- ✓ les établissements de santé des Armées
- ✓ les associations présentes en milieu hospitalier

La commission des systèmes d'information sur les établissements de santé :

- ✓ est chargée de faire des propositions et d'émettre des avis sur les questions relatives à l'échange d'informations entre les établissements de santé publics et privés, les ARH[4], les ministres de la santé et de la SS[5] et les organismes d'assurance maladie (art. R710-5-12)
- ✓ est chargée de l'élaboration et de la mise en œuvre d'un système commun d'information entre les ARH, les ministres de la santé et de la SS et les organismes d'assurance maladie (art. R710-5-12)
- ✓ sa composition et son fonctionnement sont définis aux art. R710-5-13 et 14
- ✓ est informée par les ministres de la santé et de la SS et les organismes d'assurance maladie des caractéristiques et des perspectives d'évolution de leurs SI[6] (art. R710-5-15)
- ✓ établit et rend public annuellement un rapport analysant l'état et les perspectives d'évolution des SI respectifs des ministres de la santé et de la SS et les organismes d'assurance maladie (art. R710-5-16)
- ✓ propose au travers de ce rapport les améliorations sur (1) les conditions de transmission des informations entre les établissements de santé publics et privés, les ARH, les ministres de la santé et de la SS et les organismes d'assurance maladie et (2) la politique de diffusion des données des SI respectifs ou commun (Arct. R710-5-16)

Le conseil d'administration des établissements de santé :

- ✓ définit la politique générale de l'établissement (art. L6143-1), qui décrit le projet d'établissement, qui inclut les objectifs généraux de l'établissement, dans le domaine […] du système d'information (art. L6143-2)
- ✓ sa composition est définie à l'art. L6143-5

Le Directeur des établissements de santé :

- ✓ représente l'établissement en justice et dans tous les actes de la vie civile (art. L6143-7)
- ✓ met en œuvre la politique définie par le conseil d'administration (art. L6143-7)

Plusieurs établissements, centres et professionnels de santé peuvent coopérer (art. L6134-1). S'ils constituent un réseau de santé :

- ✓ ils doivent définir une « charte du réseau » qui établit les modalités de partage de l'information dans le respect du secret professionnel et des règles déontologiques propres à chaque acteur (art. D766-1-4)
- ✓ ils doivent signer une convention constitutive qui précise l'organisation du SI et l'articulation avec les SI existants, le cas échéant, le responsable du SI (art. D766-1-5)

Les universités de formation et de recherche de médecine et de pharmacie et les hôpitaux situés dans une même ville organisent conjointement les services en centres hospitaliers et universitaires (art. 6142-3) :

- ✓ les hôpitaux et les universités sont tenus de conclure des conventions précisant la structure et les modalités de fonctionnement des centres hospitaliers et universitaires (art. 6142-3)
- ✓ le directeur des unités de formation et de recherche a qualité pour signer ces conventions, elles

doivent être soumises à l'approbation du président de l'université (art. 6142-7)
- ✓ un comité de coordination hospitalo-universitaire est obligatoirement consulté sur les choix en matière de priorité des équipements hospitaliers et universitaires (art. 6142-13)

Les associations qui organisent l'intervention de bénévoles dans les établissements de santé doivent conclure avec l'établissement concerné une convention qui détermine les modalités de cette intervention (art. L1112-5).

Les hôpitaux des Armées sont placés sous l'autorité du ministre de la Défense […] et concourent au service public hospitalier. Les ministres de la Défense et de la Santé établissent conjointement la liste des hôpitaux des Armées qui peuvent dispenser des soins (art. L6147-7)

Pour compléter les modalités de cette organisation propre à la Santé Publique, le législateur prend certaines dispositions quant à la mise en œuvre de l'obligation de maintenance et du contrôle de qualité :

- ✓ l'agence française de sécurité sanitaire des produits de santé arrête la liste des dispositifs médicaux soumis à l'obligation de maintenance, au contrôle qualité interne et au contrôle qualité externe (art. D665-5-3)
- ✓ les obligations de l'exploitant des dispositifs médicaux sont définies à l'art. D665-5-5. Elles concernent :
  - la tenue d'un inventaire des dispositifs
  - la définition et l'organisation de la maintenance et des contrôles qualités
  - le suivi des opérations de maintenance et de contrôle qualité
- ✓ les contrôles qualité externes sont réalisés par des organismes agréés (art. D665-5-6 à 12)
- ✓ le champ d'application des ces contrôles et les définitions relatives à la maintenance des dispositifs médicaux sont soumis aux art. D665-5-1 à 4
- ✓

Traitement des informations médicales et personnelles

Le traitement des informations médicales et personnelles, prévu par le code de la santé publique couvre :

- ✓ les conditions générales de transmission et d'échange des informations que les établissements de santé publics et privés sont tenus de transmettre aux ARH, aux services des ministres de la santé et de la SS, aux organismes d'assurance maladie
- ✓ les accès par des tiers au système commun d'information de l'Etat, des ARH et des organismes d'assurance maladie
- ✓ le maintien du secret médical lors de l'évaluation et de l'accréditation des établissements de santé
- ✓ l'information des personnes accueillies dans les établissements de santé et la communication des informations de santé
- ✓ le droit de la personne au respect de sa vie privée et du secret des informations la concernant
- ✓ les droits d'accès à l'information des personnes malades et des usagers du système de santé
- ✓ le contenu et les restrictions portant sur l'échange de données du dossier patient
- ✓ les règles communes d'exercice de la profession relatives à l'utilisation à des fins de prospection et de promotion commerciale de fichiers de prescription et d'informations médicales s'ils permettent d'identifier le professionnel prescripteur

Informations liées au système commun

Pour les conditions générales de transmission et d'échanges des informations :

- ✓ les ministres de la santé et de la SS :
  - définissent par arrêté la nature, le degré de précision, la périodicité et les modalités de recueil et de transmission des informations mentionnées à l'art. L710-7 (art. R710-5-17)
  - déterminent par arrêté les définitions et nomenclatures communes de données, les

caractéristiques de modules d'informations communs (art. R710-5-18)

- ✓ lorsque les données relevant du système commun d'information ou des échanges d'informations sont nominatives, elles sont rendues anonymes avant tout échange ou partage (art. R710-5-18)
- ✓ à ce sujet, les arrêtés des ministres de la santé et de la SS sont revus par la commission des systèmes d'information, qui donne son avis et doit être informée, le cas échéant, par les ministres des motifs qui les ont conduits à ne pas suivre cet avis (art. R710-5-19)

Concernant l'accès des tiers au système commun d'information :

- ✓ les informations qui doivent être partagées sur le système commun d'information sont communicables à toute personne physique ou morale dans les conditions définies par la loi n°78-753 du 17 juillet 1978 (art. R710-5-20)
- ✓ les données concernant les personnes physiques ne peuvent être communiquées que sous forme de statistiques agrégées et d'informations constituées de telle sorte que ces personnes ne puissent être identifiées (art. R710-5-21)
- ✓ les modalités de communication de ces données sont fixées par les ministres de la santé et de la SS après avis de la commission des systèmes d'information et la CNIL (art. R710 –5-21)
- ✓ les services et organismes chargés de la communication des informations ne sont pas tenus de satisfaire les demandes de communication manifestement abusives par leur nombre ou leur caractère systématique (art. R710-5-22)

Accréditation et secret médical

Les visites d'évaluation pour l'accréditation des établissements de santé sont conduites dans le respect du secret professionnel. Les experts chargés de ces visites, peuvent se voir communiquer tout document nécessaire à leur analyse. Les experts ou agent médicaux peuvent consulter sur leur demande des dossiers ou documents médicaux rendus anonymes (art. R710-6-4)

Accueil des personnes en établissement - Informations et Communications

Responsabilités de l'établissement :

- ✓ Toute personne a accès aux informations concernant sa santé. Ces informations sont définies plus précisément à l'art. L1111-7.
- ✓ Le directeur de l'établissement doit veiller à ce que toutes les mesures soient prises pour assurer la communication des ces informations (art. R1112-1).
- ✓ Ces informations sont communiquées par le médecin responsable de la structure concernée par le patient ou par un membre du corps médical désigné par lui à cet effet (art. R1112-1)
- ✓ A la fin du séjour hospitalier les éléments utiles à la continuité des soins sont transmis directement au patient au moment de sa sortie ou à un praticien désigné par le patient ou à l'autorité parentale (art. R1112-1)
- ✓ Un médecin désigné par le malade peut se voir communiquer toutes les informations concernant l'état du malade. Cette communication est assurée par le chef du service d'accueil du malade (art. R1112-6)

Archivage :

- ✓ Pour les établissements publics ou privés participant au service public hospitalier, les informations concernant la santé des patients sont conservées conformément à la réglementation relative aux archives publiques hospitalières (art. R1112-7).
- ✓ Dans les établissements privés ne participant pas à l'exécution du service public hospitalier, ces informations sont conservées sous la responsabilité d'un ou de plusieurs médecins désignés à cet effet par la conférence médicale (art. R1112-7).
- ✓ Dans tous les cas, le directeur de l'établissement veille à ce que les dispositions soient prises pour assurer la garde et la confidentialité des informations de santé conservées (art. R1112-7).
- ✓ Lorsqu'un établissement privé, ne participant pas à l'exécution du service public hospitalier,

cesse son activité, les informations de santé de ses patients peuvent faire l'objet d'un don à un service public d'archive (art. R1112-8).

Echange de données électroniques :

- ✓ Lorsque des cartes électroniques sont utilisées pour assurer la confidentialité des échanges d'informations contenues dans le dossier du patient définies à l'art. R1112-2, ces cartes doivent être conformes aux dispositions des art. R161-52 à 54 du code de la SS (art. R1112-7).

Droit des personnes :

- ✓ Le droit de la personne est essentiellement pris en compte par la loi du 4 mars 2002. Des notions telles que l'accueil du patient ou sa désignation de personnes de confiance y sont précisément définies. Se rapporter à la fiche de lecture associée. On pourra retenir l'art. L1111-4 qui présente l'essentiel.
- ✓ Sont définis par l'art. L1111-4 de la loi du 4 mars 2002, les éléments relatifs au droit de la personne suivants :
- Les conditions d'accès aux informations concernant sa santé, leur durée et les modalités de conservation sont mentionnées dans le livret d'accueil du patient prévu à l'art. L1112-2
- Toute personne prise en charge […] a droit au respect de sa vie privée et du secret des informations la concernant
- Hors dérogation, le secret couvre : les informations de la personne venues à la connaissance du professionnel de santé, de tout membre du personnel et de toute personne en relation, par ses activités, avec l'établissement
- Deux (ou plus) professionnels de santé peuvent échanger ces informations « sauf opposition de la personne dûment avertie », afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire
- Si la personne est prise en charge par une équipe, les informations la concernant sont réputées confiées par le malade à l'ensemble de l'équipe
- Pour garantir la confidentialité des informations, leur conservation sur support informatique ou leur transmission par voie électronique entre professionnels sont soumises à des règles définies par décret en Conseil d'état, après avis de la CNIL. Ce décret détermine les cas où l'utilisation de la CPS[7] est obligatoire
- En cas de diagnostic grave et sauf opposition du malade, le secret médical ne s'oppose pas à ce que ces informations soient communiquée aux proches, à la famille, à la personne de confiance
- En cas de décès, le secret médical ne s'oppose pas à ce que ces informations soient délivrées aux ayants droit pour connaître la cause de la mort, défendre la mémoire du défunt, etc.
- Obtenir des informations en violation du présent art. est puni d'un an d'emprisonnement et de 15 k€ d'amende
- ✓ L'art. L1511-3, définit pour les territoires d'outre-mer (Mayotte), des conditions particulières d'application du droit des malades et des usagers du système de santé :
- L'établissement public est tenu de communiquer aux personnes ayant reçu des soins, sur leur demande et par l'intermédiaire du praticien qu'elles désignent les informations médicales de leur dossier
- Les praticiens qui ont prescrit l'hospitalisation ont accès, sur leur demande, à ces informations
- Les médecins membres de l'inspection générale des affaires sociales, les médecins inspecteurs de la santé publique et les médecins conseils des organismes d'assurance maladie ont accès, dans le respect de la déontologie médicale, à ces informations si elles sont nécessaires à l'exercice de leur mission

Dossier du patient :

- ✓ L'art. R1112-2 précise la constitution du dossier médical du patient (établissements publics ou privés). On distingue 3 classes d'informations :
- 1ère classe d'informations : elles sont recueillies lors de consultations externes dispensées dans l'établissement, lors de l'accueil au service des urgences ou au moment de l'admission et au cours du séjour. Pour la sécurité du patient on pourra retenir : la recherche d'antécédents et de

facteurs de risques, les conclusions de l'évaluation clinique initiale, la nature des soins dispensés et les prescriptions établies (consultations externes et urgences), les actes transfusionnels pratiqués, les soins dispensés par les autres professionnels de santé, les correspondances échangées

- 2nde classe d'informations : elles sont établies à la fin du séjour et comportent notamment le compte-rendu d'hospitalisation et la prescription de sortie
- 3ème classe d'informations : elles ont été recueillies auprès de tiers n'intervenant pas dans la prise en charge thérapeutique

✓ le protocole d'anesthésie, les informations recueillies lors de l'intervention et lors de la surveillance, ainsi que les consignes données au personnel qui accueille le patient en hospitalisation, sont classés au dossier du patient et transmis par écrit (art. D712-50)

✓ Seules les informations des 1ère et 2nde classe sont communicables (art. R1112-2).

✓ D'après l'art. R1112-3, le dossier comporte les éléments d'identification suivants :

- L'identification du patient et le cas échéant de la personne de confiance et de la personne à prévenir
- Chaque pièce est datée et comporte l'identité du patient, ainsi que l'identité du professionnel de santé qui a recueilli ou produit les informations
- Les prescriptions médicales sont horodatées et signées – le nom du médecin est inscrit en caractères lisibles
- L'identité du patient comporte les éléments suivants : nom – prénom – date de naissance ou n° d'identification

✓ Si le praticien prescripteur de l'hospitalisation demande communication du dossier du patient, elle doit être soumise à l'accord du patient ou de l'autorité parentale ou des ayants droits en cas de décès (art. R1112-4)

Règles communes d'exercice de la profession :

✓ Il est précisé à l'art. L4113-7 que sont interdites la constitution et l'utilisation à des fins de prospection ou de promotion commerciales de fichiers composés de données relatives aux prescriptions médicales ou d'informations médicales mentionnées à l'art. L161-29 du code de la SS, dès lors que ces informations permettent d'identifier directement ou indirectement le professionnel prescripteur

✓ La constitution et l'utilisation de tels fichiers sont punies de 2 ans d'emprisonnement et de 500kF d'amende

Informations relatives aux centres de santé :

✓ Les centres de santé doivent établir annuellement un rapport d'activité comportant toutes informations non nominatives relatives à la clientèle du centre (art. D765-6)

Disponibilité du système d'information

Les aspects liés à la disponibilité du système d'information ne sont pas traités directement.

Néanmoins, les conditions techniques de fonctionnement de certaines unités ou structures de soins, laissent à penser qu'il pourrait être nécessaire d'assurer un accès permanent et continu aux données et aux services du système d'information de ces structures.

D'après notre compréhension du code, cela couvrirait :

✓ les unités d'anesthésie
✓ les unités de réanimation
✓ les unités de soins intensifs
✓ les unités d'accueil et de traitement des urgences
✓ les structures d'hospitalisation à domicile

Les unités d'anesthésie doivent permettre d'assurer une surveillance clinique continue lors de la prise en charge du patient (art. D712-43).

Les unités de réanimation doivent permettre d'assurer 24/7[8] une permanence médicale (art. D712-105).

Les unités de soins intensifs (art. D712-122) et les unités d'accueil et de traitement des urgences (art. D712-57 à 60) doivent disposer 24/7 de moyens techniques et organisationnels propres à leurs activités.

Les structures d'hospitalisation à domicile doivent disposer d'un système de communication à distance permettant d'assurer 24/7 une liaison permanente avec les patients, leurs familles, le personnel médical (art. D712-35).

Commentaires

Concernant le concept de responsable de la sécurité …

L'organisation relative au système d'information de santé, telles qu'elle est définie par le code de la santé publique, permet de définir un 1er niveau de responsabilités vis-à-vis de la sécurité de l'information.

Tout d'abord on doit distinguer deux systèmes d'information : (1) le SI commun sur les établissements de santé, (2) les SI propres à chaque établissement, aux réseaux de soins, aux centres hospitalier et universitaires, aux établissements des Armées.

Pour le 1er SI, les responsabilités en matière de sécurité sont clairement attribuées aux ministères de la santé et de la SS. Ces responsabilités requièrent la consultation de la commission des systèmes d'information sur les établissements de santé. Celle-ci dispose de responsabilités quant à la recommandation et au suivi des pratiques et dispositifs à mettre en œuvre. Le périmètre de ces responsabilités couvre la transmission des informations entre établissements de santé et les autres organismes (CNAM, Ministères, ARH).

Pour le 2nd type de SI, les responsabilités se répartissent entre le conseil d'administration (qui décide) et le Directeur d'établissement (qui met en œuvre). Lors de la coopération entre établissements, qu'il s'agisse d'établissements publics ou privés, d'unités de formation universitaires, d'hôpitaux des Armées ou de l'intervention d'associations au sein des établissements, des conventions doivent être signées. En revanche il n'est pas explicitement mentionné que ces conventions doivent traiter des aspects liés à l'emploi des SI, donc à leur sécurité. Toutefois, en ce qui concerne le cas particulier des réseaux de santé il est clairement spécifié que les entités qui y participent doivent établir une convention qui précise l'organisation du SI et l'articulation avec les SI existants, ainsi qu'une charte qui établit les modalités de partage de l'information. Ce qui touche directement à la sécurité des SI.

Par ailleurs, d'un point de vue opérationnel, les dispositifs médicaux sont soumis à des obligations de maintenance et de contrôle qualité dont les modalités sont décrites avec précision. La liste de ces dispositifs est établie par l'agence française de sécurité sanitaire. Reste à savoir dans quelles mesures, tout ou partie du SI peut (ou pourrait) être intégré à cette liste. Il pourrait alors s'agir d'en contrôler le niveau de sécurité comme partie intégrante de la qualité du service rendu. Ce point nécessite certainement d'être traité de manière plus approfondie …

Au travers de ces articles, des responsabilités en matière de sécurité se dessinent, mais ne sont pas explicitement définies. Ces éléments devraient permettre d'envisager les responsabilités en matière de sécurité en cohérence avec le code de la santé. C'est la limite du texte. Cela mériterait certainement d'être approfondi en fonction d'un retour d'expérience relatif aux pratiques « du terrain ».

Concernant le concept de respect de la vie privée …

Sur ce sujet, les textes sont précis. Echange d'informations entre praticiens, diffusion de données médicales sur le SI commun des établissements de santé, informations fournies à l'accueil du patient, contenu de son dossier médical, … le respect de la vie privée est largement abordé. Il se définit selon trois composantes :

- ✓ le respect de la confidentialité des informations médicales et personnelles,
- ✓ le droit à l'information,
- ✓ les règles liées à la conservation et à l'échange de données.

Le respect de la confidentialité des informations médicales et personnelles concerne :

- ✓ l'anonymisation des informations liées aux PMSI(s) et aux rapports d'activités des centres de santé

- ✓ les obligations de secret professionnel et médical des professionnels de santé qui interviennent avant, pendant ou après la prise en charge du patient :
- directeur d'établissement
- praticiens prescripteurs
- médecins traitants
- équipe médicale et administrative
- experts ou agents « mandatés » pour des évaluations ou autres expertises

Les dérogations à ces obligations sont généralement applicables dans les cas suivants :

- ✓ assurer la continuité des soins dans l'intérêt du patient
- ✓ garantir les droits à l'information des ayants droit en cas de décès
- ✓ accompagner le patient lors de diagnostics graves

Il est intéressant de noter que le respect de la confidentialité des données protège les patients, mais aussi les professionnels de santé en tant qu'auteurs de ces informations. C'est ce qui apparaît lorsqu'il est explicité qu'il est interdit de constituer, à des fins commerciales, des fichiers de données relatives aux prescriptions médicales et permettant d'identifier les médecins prescripteurs.

Le droit à l'information est traité « à part égale » du droit au respect de la confidentialité. Il couvre les obligations des professionnels de santé à informer le patient lors de son accueil à l'établissement, au cours de sa prise en charge et à l'issue du traitement afin d'assurer la continuité des soins, de lui faire valoir ses droits d'accès à l'information et plus largement dans le respect de sa vie privée (eg. connaître son état de santé).

Pour ce qui est des règles de conservation des données, les établissements publics ou privés, participant au service public hospitalier, doivent traiter ces informations conformément à la réglementation sur l'archivage public hospitalier. Reste à savoir ce dont il s'agit … Ce point mériterait certainement d'être approfondi.

Quant à l'échange des données il est exclusivement traité avec précision pour l'emploi de cartes CPS avec l'assurance maladie.

Pour tous ces points, il est à noter que c'est le Directeur d'établissement qui a la responsabilité de s'assurer que les moyens nécessaires sont mis en œuvre et appliqués.

Concernant les autres concepts …

Le code de la santé, lorsqu'il évoque la sécurité des informations, traite avant tout des aspects de confidentialité de ces informations. Pour cette première lecture peu d'éléments semblent traiter, directement du moins, des aspects d'intégrité, d'auditabilité et de disponibilité des informations. Pourtant l'application de ces notions est une garantie essentielle de la sécurité du patient …

Néanmoins, l'identification du contenu du dossier du patient laisse penser :

- ✓ que la disponibilité et l'intégrité des données qu'il contient sont essentielles à la qualité et notamment à la continuité des soins
- ✓ que l'authenticité du patient pourrait être importante : son identification au niveau du dossier et pour chaque pièce qu'il contient est-elle et peut-elle être simplement <u>présumée</u> ?
- ✓ que la preuve des prescriptions peut être requise : les prescriptions médicales doivent être signées par le médecin prescripteur et porter son nom en caractères lisibles

En outre, les conditions techniques de fonctionnement de certaines unités ou structures de soins semblent nécessiter un accès permanent et continu aux moyens de traitement et de prise en charge. Dans quelles mesures le SI de santé est-il nécessaire à la satisfaction de ces conditions techniques ? Ne

touche-t-on pas là à des exigences relatives à la disponibilité du SI, notamment au besoin de veille ou d'astreinte des équipes informatiques ?